



**BCM50 RIs 6.0**

# **System Start Up**

**Task Based Guide**

**Copyright © 2010 Avaya Inc.  
All Rights Reserved.****Notices**

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

**Documentation disclaimer**

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

**Link disclaimer**

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

**Warranty**

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: <http://www.avaya.com/support>

Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

**Licenses**

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://support.avaya.com/licenseinfo/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

**Copyright**

Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

**Third Party Components**

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/Copyright>.

**Trademarks**

*The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.*

**Downloading documents**

For the most current versions of documentation, see the Avaya Support. Web site: <http://www.avaya.com/support>

**Contact Avaya Support**

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://www.avaya.com/support>

Copyright © 2010 ITEL, All Rights Reserved

The copyright in the material belongs to ITEL and no part of the material may be reproduced in any form without the prior written permission of a duly authorised representative of ITEL.

## Table of Contents

<b>System Start Up .....</b>	<b>6</b>
Overview .....	6
Required Information .....	6
Standalone .....	6
LAN Connection .....	7
WAN Connection .....	8
Flow Chart .....	9
Obtaining a Keycode File .....	10
PC Configuration .....	11
Physical Connection to the BCM .....	12
Testing the IP connection using Ping .....	12
Installing the Element Manager Application .....	13
Element Manager Connection to the BCM .....	19
Software Keycodes .....	21
Configuring the LAN IP Address .....	24
Configuring DHCP .....	28
Setting the System Name .....	31
Setting the Date and Time .....	32
Setting the Start DN and Telephony Region .....	34
Initialising CallPilot Manager .....	36
Media Bay Modules .....	38
Media Bay Module Configuration .....	38
Configuring the Media Bay Modules .....	38
Trunk Media Bay Modules .....	39
PRI Modules .....	39
DASS2 Modules .....	46
DPNSS Modules .....	50
BRI Module .....	53
CTM/GATM (4 and 8 port) Module .....	56
Station Media Bay Modules .....	58
DSM 16/32 Modules .....	59
ASM Analog Station Module Configuration .....	61
Combination Modules .....	62
Connecting the BCM to the Network .....	65

Registering IP Terminals..... 65

**Additional Information..... 67**

Startup Profile Configuration Tool..... 67

    Before Configuring the Startup Profile Configuration Tool ..... 67

    Obtaining the Startup Profile Configuration Tool ..... 69

    Startup Profile Settings ..... 74

    Running the Startup Profile..... 79

    Next Step ..... 80

Keycode Credit System ..... 80

**Avaya Documentation Links ..... 82**

# System Start Up

## Overview

This guide details the steps required to set the BCM to a basic working state. When the procedures described in this document have been applied the BCM will be able to perform basic call operations, and the system will then be ready for further configuration such as Telephony Services, Contact Centre, etc.

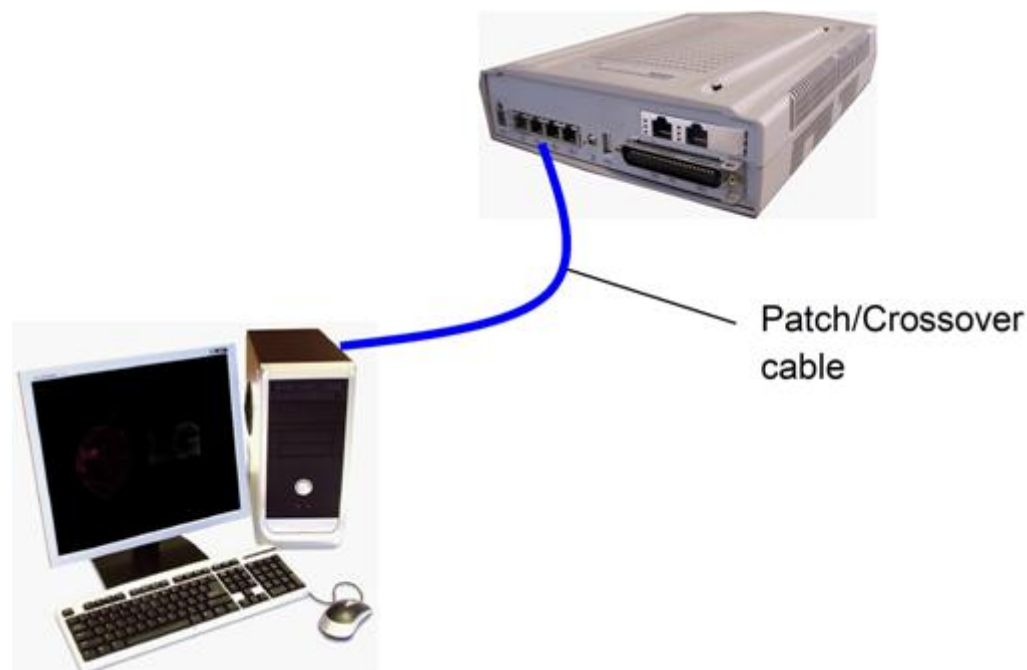
It is assumed that the BCM has been installed and connected to a power supply before starting this guide.

## Required Information

Obtain the following parameter values from the customer's network administrator. The information required depends on what type of network the BCM is to be installed in.

### ***Standalone***

In this situation, the BCM is connected directly to a PC.



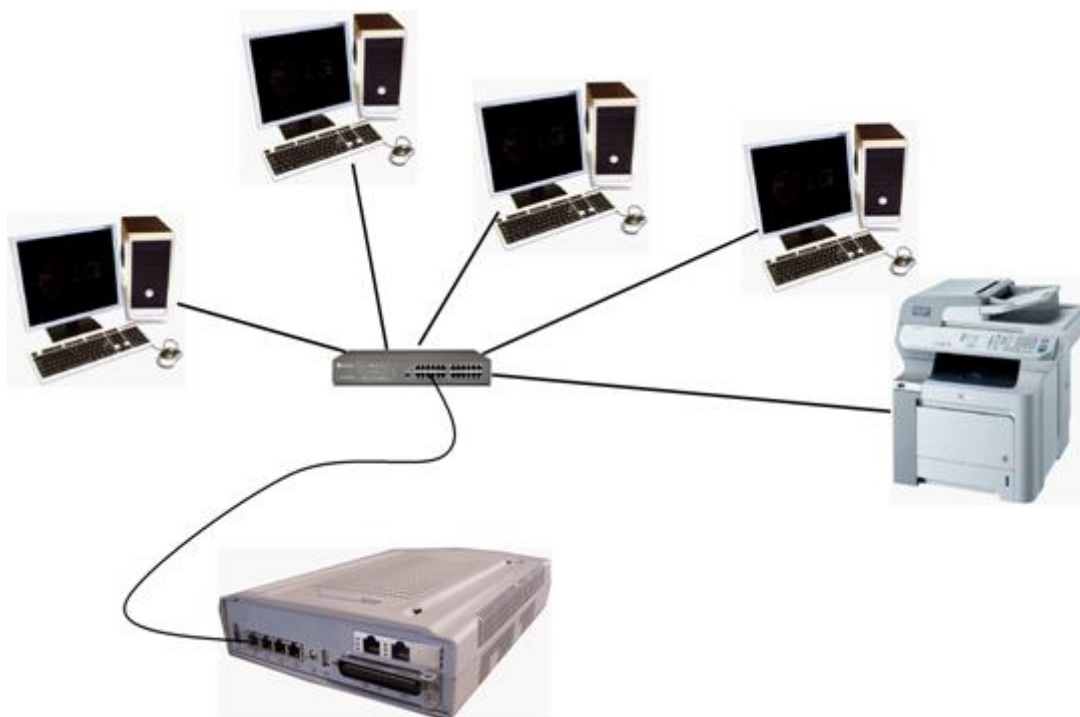
The required information for this situation would be:

- BCM System ID
- BCM Name
- Telephony Region
- Time Zone
- Time Source

- DHCP On/Off?
- License File (Keycode File)
- Telephony Template
- Start DN of the system
- Public/Private Received digits
- CallPilot Region
- CallPilot Password
- CallPilot User Interface (UI) Style
- CallPilot Attendant DN
- Lines to assign to CallPilot Auto-Attendant

### ***LAN Connection***

In this situation, the BCM is connected to a Local Area Network.



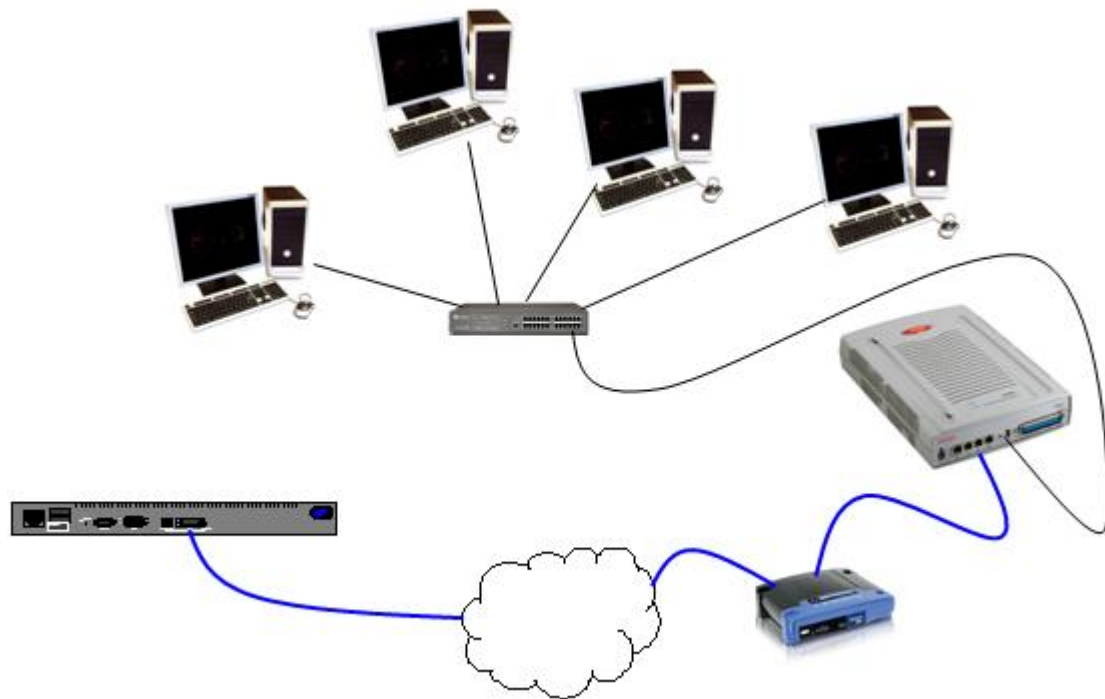
In addition to the information required for a Standalone installation, you now need the following details:

- IP Address and Subnet Mask for the BCM
- If using DHCP, Network Default Gateway,
- Domain Name of the DNS server (if the customer has a separate DNS Server)
- IP Address(es) of the DNS server (if relevant)
- IP Telephony Registration details (enable, password etc.)

## ***WAN Connection***

This scenario only relates to a BCM50(b)e installation.

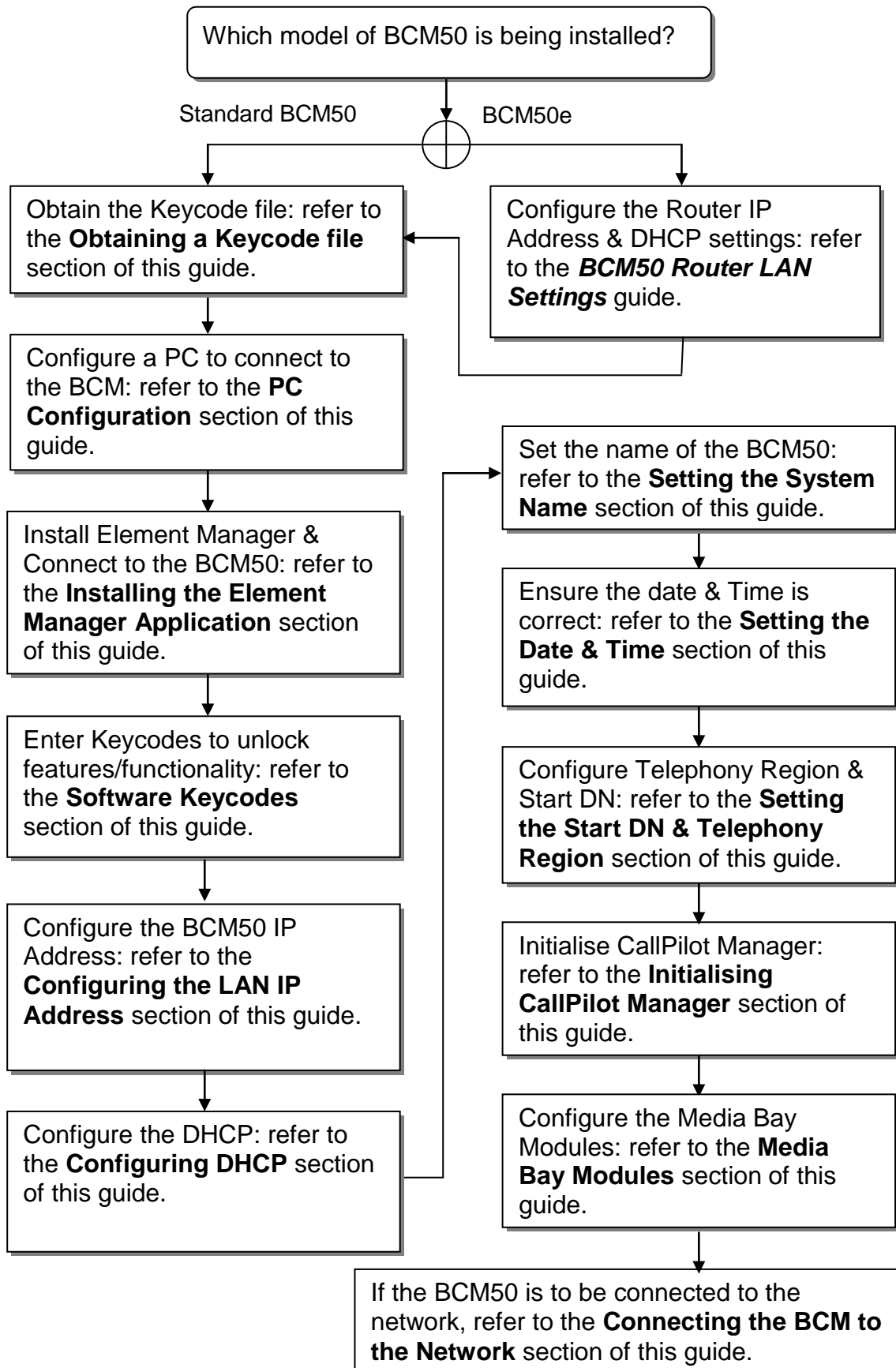
The WAN information required for BCM50(b)e models will be entered in the BCM50(b)e Wizards. Refer to the ***BCM50 Router Wizards Guide***.





## Flow Chart

The flow chart outlines the steps involved in System Start-Up:



## Obtaining a Keycode File

Keycodes unlock features and applications on the BCM. Without applying Keycodes it would not even be possible to make a telephone call!

This section describes how to obtain the Keycode file.

Keycodes are generated based on two inputs:

- The BCM System ID
- Software Authorisation Codes

Software Authorisation Codes are orderable items, and are supplied in paper form.

There are a number of ways to find the BCM System ID. To find the System ID without powering up the BCM:

1. Look on the underside of the BCM.
2. You will notice a label with three bar codes on it. The bottom bar code is the System ID and is labelled SystemID/MAC (it is linked to the MAC address of the BCM50 LAN ports).



3. Make a note of the System ID; you will need it for Keycode generation. It will also be required if you wish to use the Startup Profile Configuration Tool (refer to the **Startup Profile Configuration Tool** section of this guide for details of the Startup Profile procedure.)
4. Contact your Keycode supplier and supply the System ID and Authorisation Codes.
5. You should receive a Keycode file, which will be entered during the Start Up procedure.

## PC Configuration

The BCM50 has a dedicated OAM port. It is recommended that you perform any maintenance/configuration from this port. There are also:

- 1 x dedicated LAN Port on BCM50, & 5 x dedicated LAN Ports on BCM50e
- 2 x dual function ports that act as expansion ports for Media Bay Modules, and also LAN ports



OAM Port (10.10.11.1)

LAN Ports (192.168.1.2)

A PC/laptop can be configured to connect to the BCM OAM in two ways:

- Set your PC/laptop to obtain an IP Address automatically (preferred , as DHCP is always operating on the OAM port)
- Manually set your PC/laptop's IP Address (IP Address: 10.10.11.2, Subnet Mask: 255.255.255.252)
- (Note that the OAM port default settings are IP Address: 10.10.11.1, Subnet Mask: 255.255.255.252)

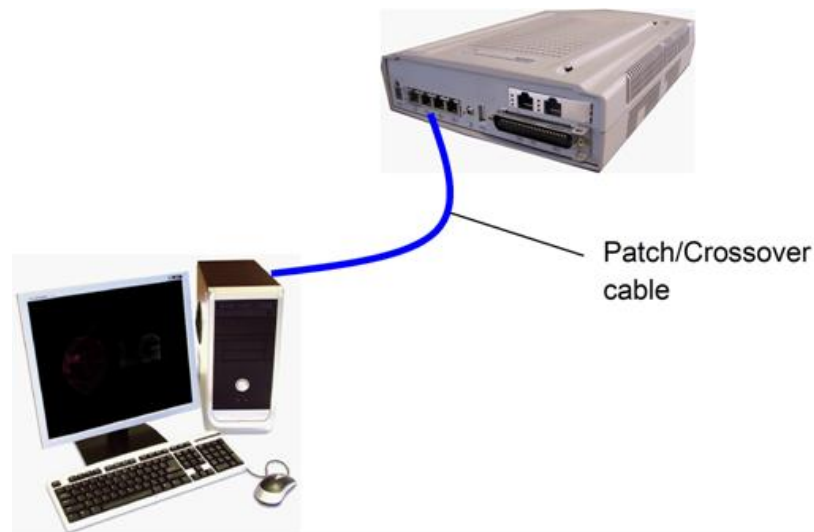
The default setting for the LAN Ports is:

- IP Address: 192.168.1.2
- Subnet Mask: 255.255.255.0

For information concerning configuring the network settings of your PC, refer to the **Networking Essentials Guide**.

### ***Physical Connection to the BCM***

The BCM50 OAM port can accommodate either a patch cable or a cross-over cable.

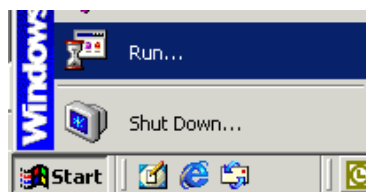


One end of the cable is connected to the PC network card, the other end to the OAM port of the BCM.

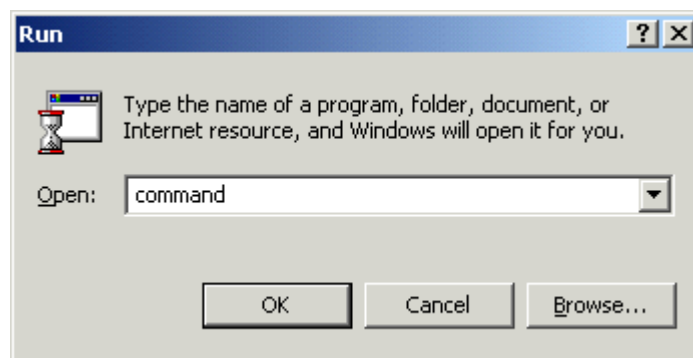
### ***Testing the IP connection using Ping***

When a physical connection has been made, you should next test the connection by “pinging” the BCM. This test is performed on the Laptop/PC that is connected to the BCM.

1. Go to the **Start** button on your Windows desktop, and select **Run**.



2. Type **command** and press **OK**. This will bring up the MS-DOS / command prompt.



3. Type **ping** followed by the default IP Address of the LAN port you are connected to (OAM = 10.10.11.1, LAN Core = 192.168.1.2). Press **Enter**.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Pauls.PSHARPLAPTOP>ping 10.10.11.1
```

4. There are differing responses that may now be displayed.
  - a. If a **Reply** is received from the BCM (as displayed below) the IP connection is working.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Pauls.PSHARPLAPTOP>ping 10.10.11.1

Pinging 10.10.11.1 with 32 bytes of data:

Reply from 10.10.11.1: bytes=32 time<1ms TTL=64
Reply from 10.10.11.1: bytes=32 time<1ms TTL=64
Reply from 10.10.11.1: bytes=32 time<1ms TTL=64
Reply from 10.10.11.1: bytes=32 time<1ms TTL=64

Ping statistics for 10.10.11.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Pauls.PSHARPLAPTOP>
```

- b. If any other response is displayed, check the IP settings of your laptop/PC and the physical connection between the laptop/PC and BCM.

## Installing the Element Manager Application

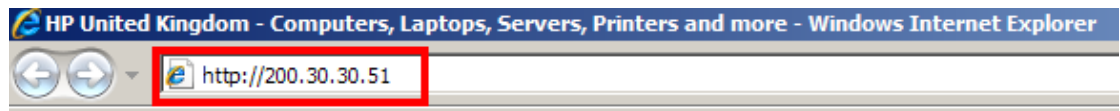
Element Manager is the application that allows configuration of the BCM via a PC/laptop.

**Note:** You must ensure you are using the correct version of Element Manager. The version supplied with the BCM will be the correct version.

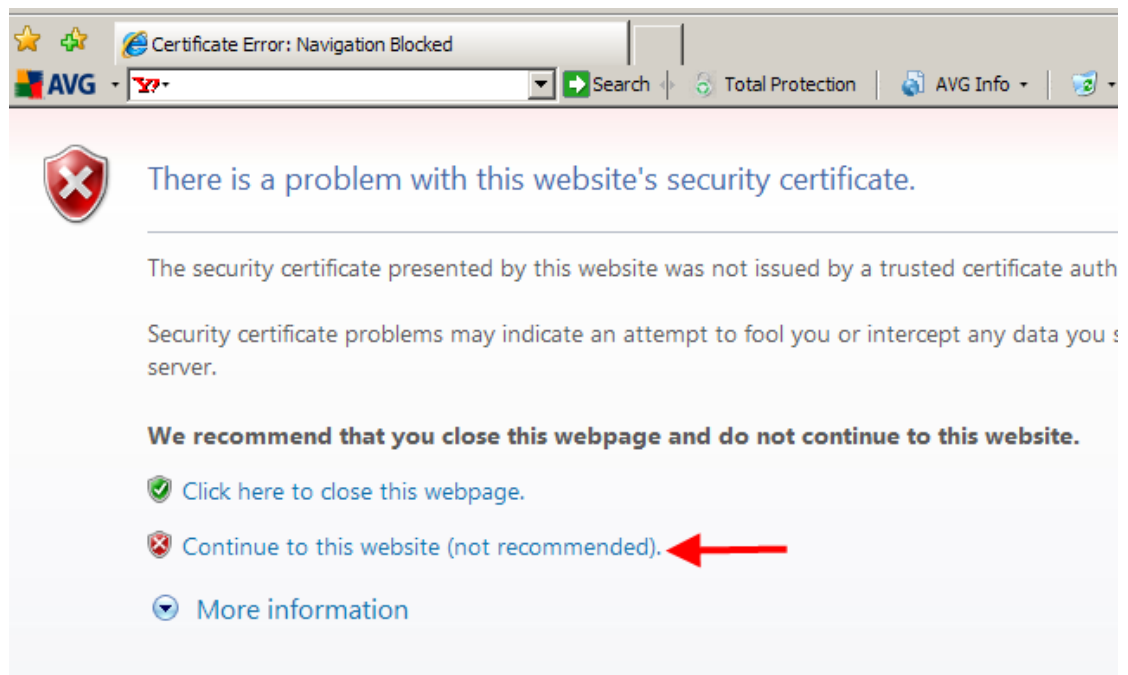
The application should be installed on the PC/laptop that is required to perform configuration.

**Note:** Java Runtime Environment must be installed on the PC used to access Application Launcher. Visit [www.java.com](http://www.java.com) to download this.

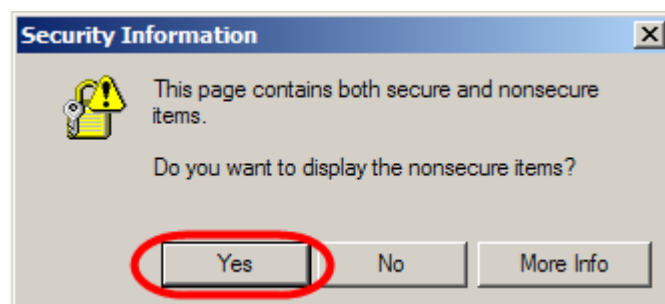
1. Point your web browser at the BCM's IP Address.



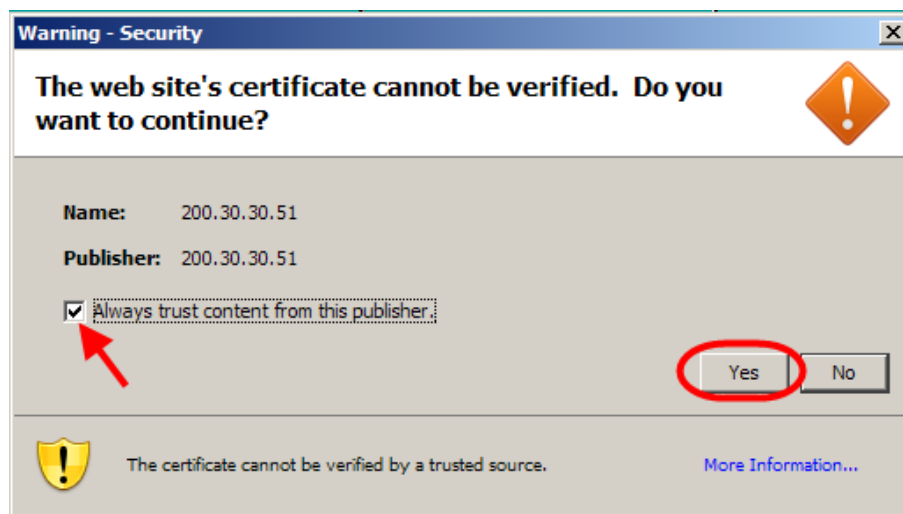
2. You may get presented with the Certificate Error window. If so, click on the **Continue to this website (not recommended)** link.



3. If you see the following information box, click **Yes**.



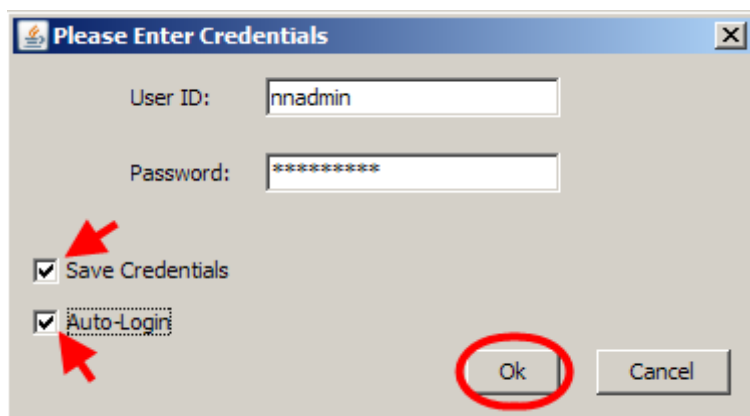
4. You may be presented with a second certificate error message. To avoid seeing the message again, tick the **Always trust content from this publisher** box, and click **Yes**.



5. Again, you may be presented with a security warning. Tick the **Always trust content from this publisher** box to avoid seeing the message in future, and click **Run**.



6. You will be asked to enter the BCM account credentials. Tick the **Save Credentials** and **Auto-Login** boxes for easier future access. Click **OK** when the account details have been entered.



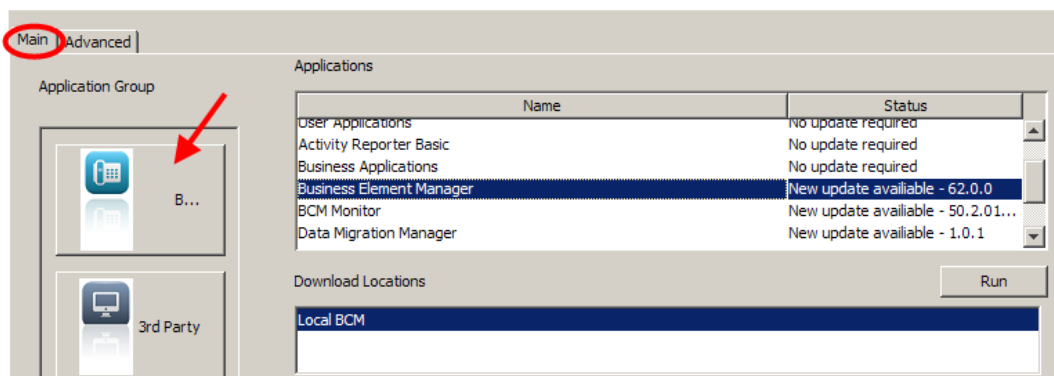
A dialog box titled "Please Enter Credentials" with a close button (X) in the top right corner. It contains two input fields: "User ID:" with the text "nnadmin" and "Password:" with masked characters "\*\*\*\*\*". Below the password field are two checked checkboxes: "Save Credentials" and "Auto-Login". At the bottom right are "Ok" and "Cancel" buttons. Red arrows point to the checkboxes, and a red circle highlights the "Ok" button.

7. In the Application Launcher window, ensure the **Main** tab is selected. Click on the **BCM** button to ensure the required list of applications are present.

Welcome

to

BCM



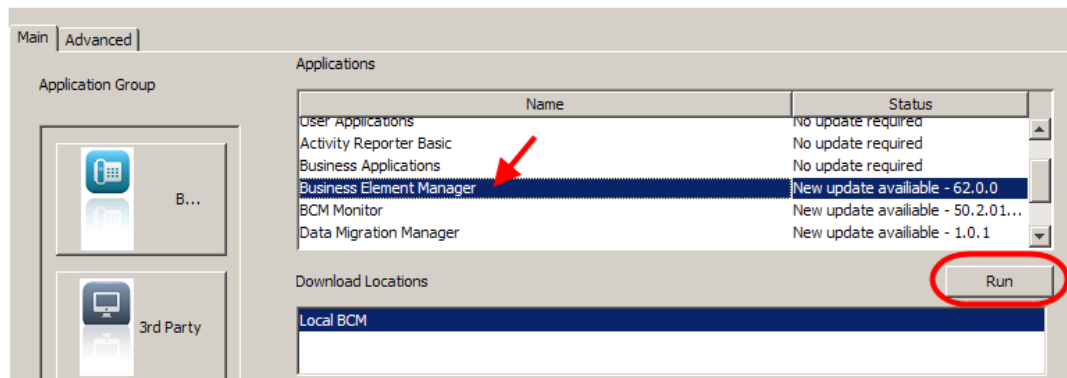
The Application Launcher window shows the "Main" tab selected (circled in red). On the left, under "Application Group", there is a "BCM" button with a red arrow pointing to it. The main area displays a table of applications with their status.

Name	Status
User Applications	No update required
Activity Reporter Basic	No update required
Business Applications	No update required
Business Element Manager	New update available - 62.0.0
BCM Monitor	New update available - 50.2.01...
Data Migration Manager	New update available - 1.0.1

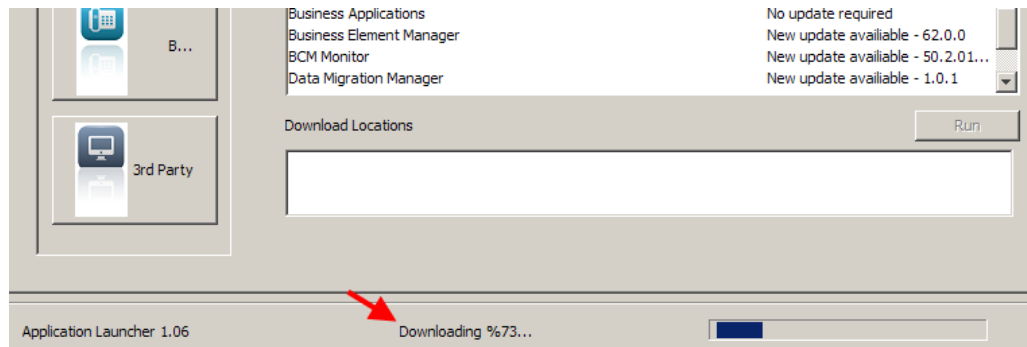
Below the table, under "Download Locations", there is a "Local BCM" entry. A "Run" button is located at the bottom right.



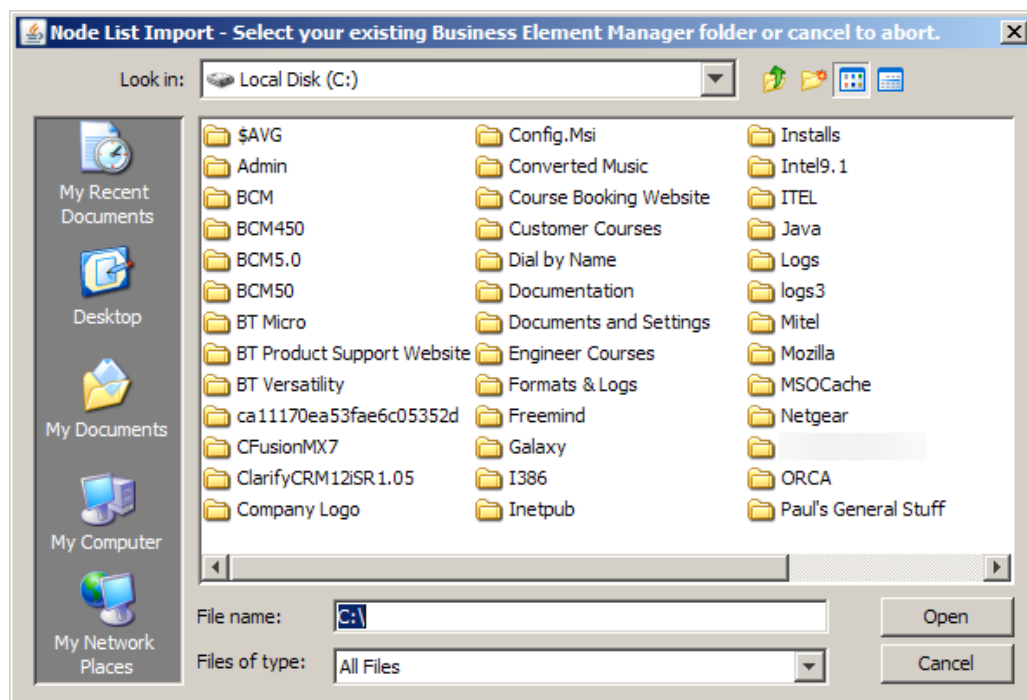
8. From the list of Applications, select **Business Element Manager** and click on the **Run** button.



9. The download progress will display.

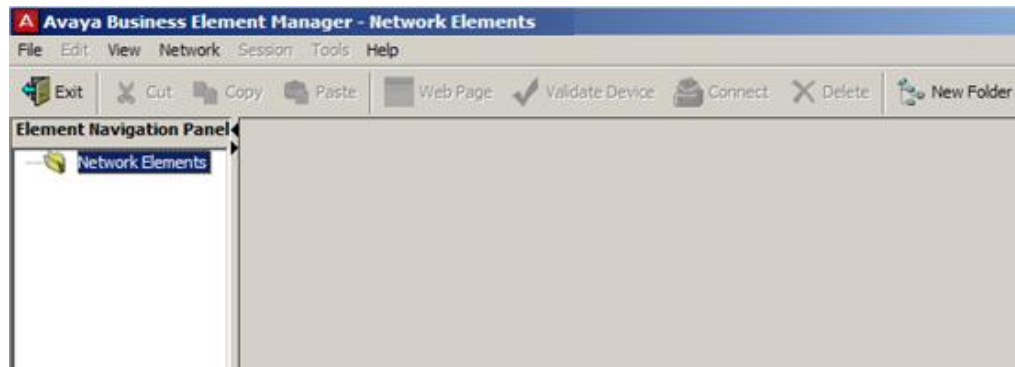


10. In the **Node List Import** window, you can browse to a folder containing a previous BEM installation (e.g. to import previous BEM nodes) and click on **Open**. Alternatively, click on **Cancel** to continue.



11. If there hasn't been a previous installation of Element Manager an "empty" version (i.e. no preconfigured settings or Elements) will be presented. If you selected a folder containing a previous installation in the last step, the existing nodes will be listed in the Element Navigation Panel.

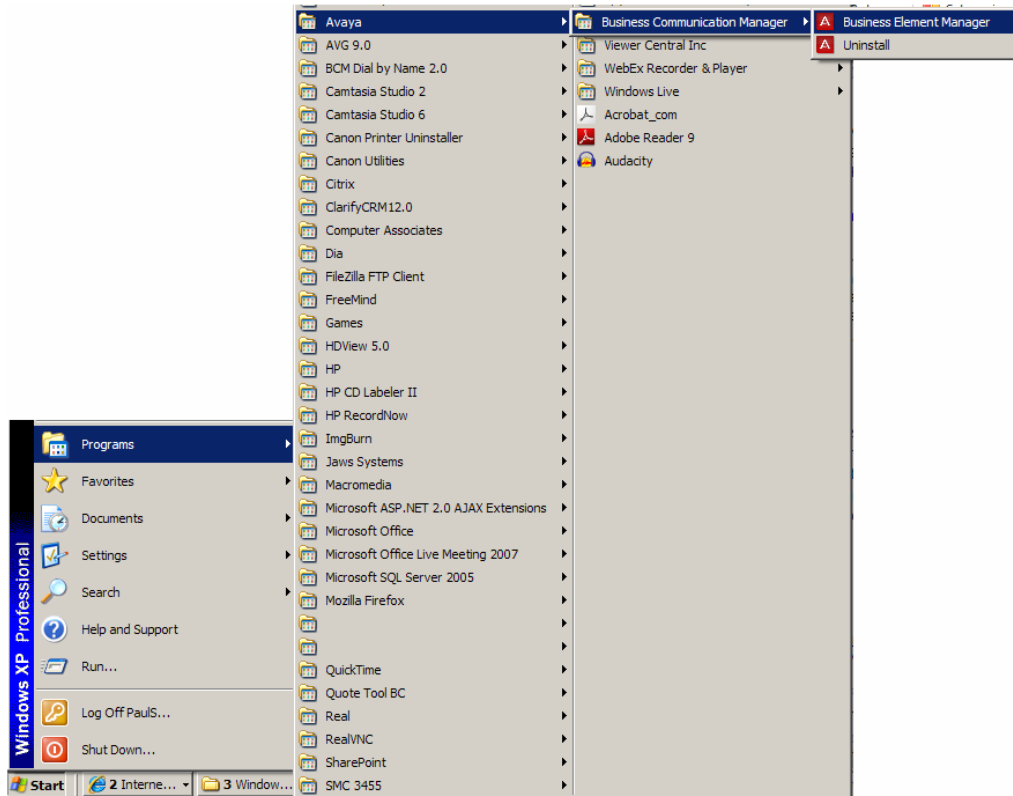
**Note:** Subsequent launches of Element Manager from Application Launcher or via Start, Programs or desktop shortcut will show configured Elements, and retain Element Manager settings.



## ***Element Manager Connection to the BCM***

To access Element Manager for configuration purposes:

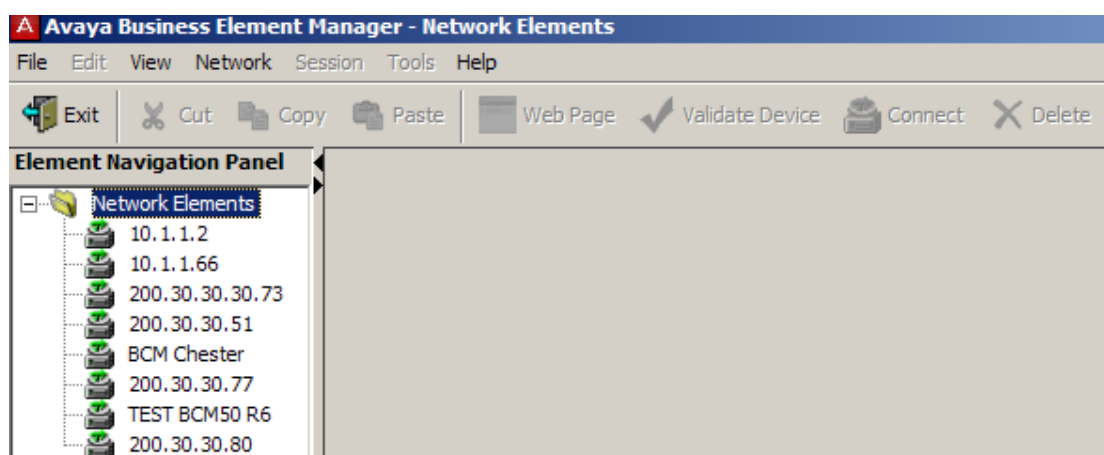
1. To access the Business Element Manager application from the Start Menu, navigate to **Start, Programs, Avaya, Business Communications Manager, Business Element Manager**.



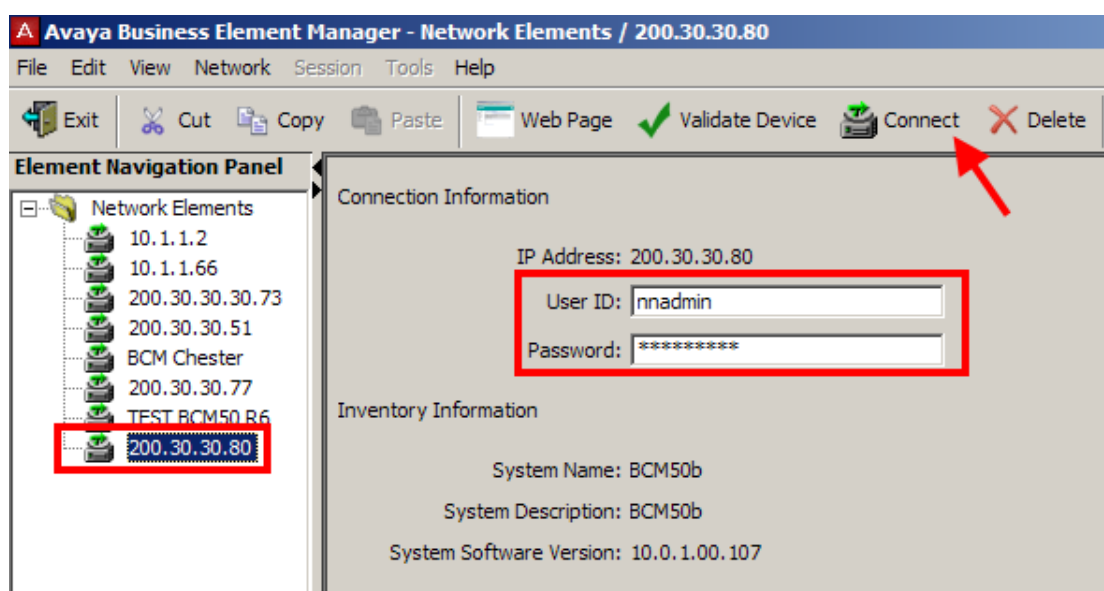
2. Alternatively, double-click on the **Business Element Manager** desktop icon.



3. You will be presented with the **Element Manager** interface.

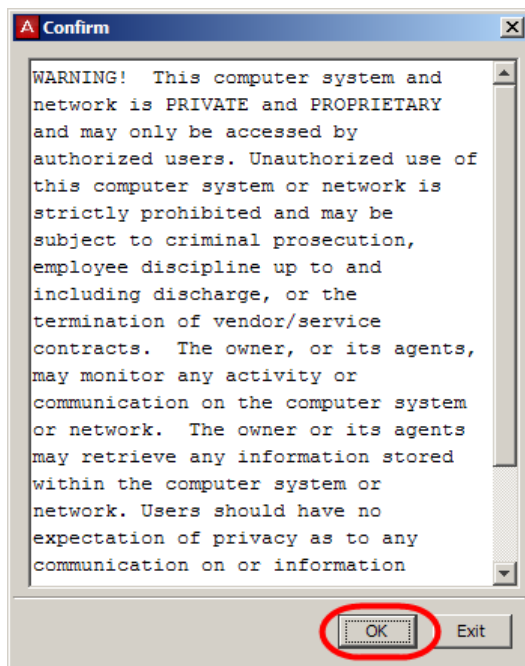


4. Open the **Network Elements** folder and select the IP Address of the BCM.

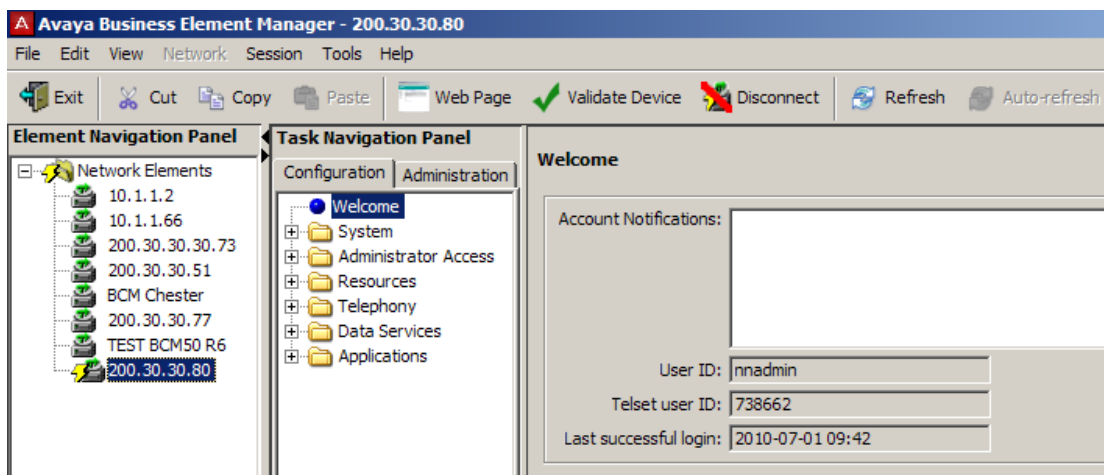


5. Enter the User Name of the BCM in the User Name field, by default this is **nnadmin**. Then enter the Password in the Password field, by default the password is **PlsChgMe!**. Click the **Connect** button.

6. A warning screen will appear, read the warning and click **OK**.



7. You will be presented with the Element Manager interface.



## Software Keycodes

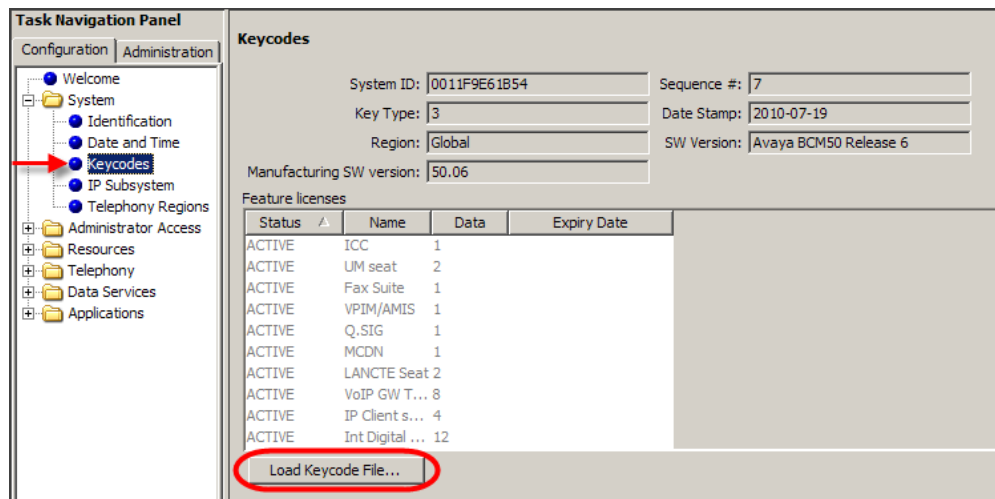
**Note:** If you have already applied the Keycodes via the Startup Profile, you can proceed to the **Initialising CallPilot Manager** section.

Keycodes are entered in the Keycodes section of Element Manager, and are entered as a file containing a range of features

**Note:** When entering the Keycode file, you may be asked to reboot the BCM. Certain features such as VoIP G/W Trunks, require the BCM to be rebooted.

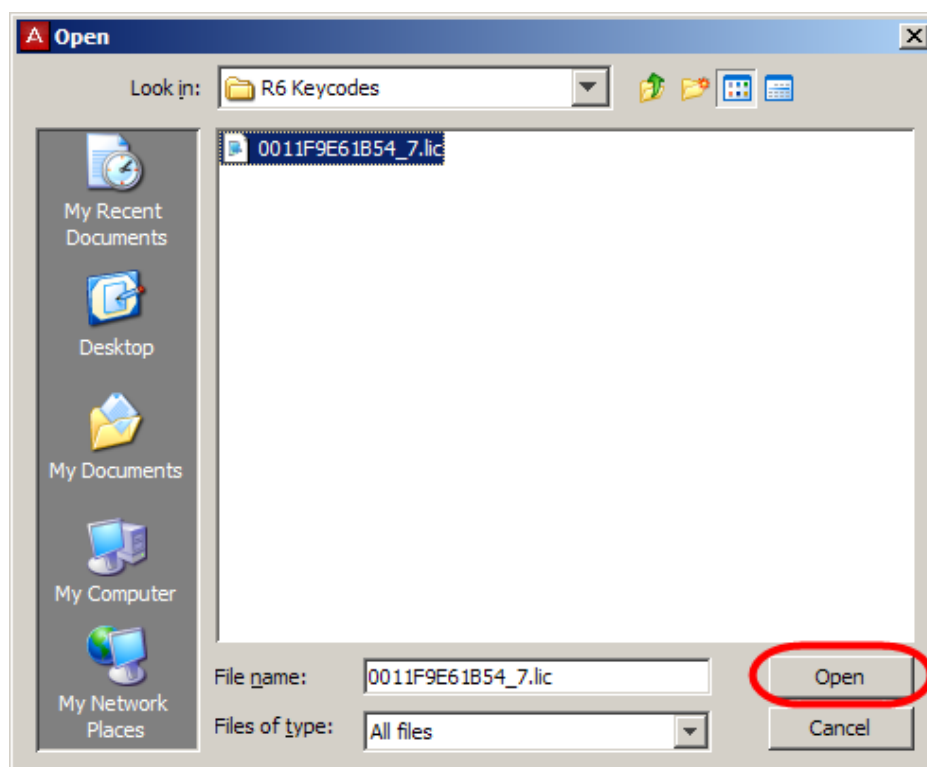
Use the following procedure to load a Keycode file.

1. Access Element Manager (refer to **Element Manager Connection to the BCM** section of this guide).
2. In Element Manager, click on the **Configuration** tab, open the **System** folder and click on **Keycodes**.
3. To load a keycode file, click on the **Load Keycode File** button.



**Note:** For new un-configured BCM systems, the Status fields will state **IDLE** and the Data fields will show a value of **0**.

4. Browse to the location of the file and select it. Click **Open**.



5. The features will be applied and viewable in the Feature Licenses table.

**Keycodes**

System ID: 0011F9E61B54      Sequence #: 7

Key Type: 3      Date Stamp: 2010-07-19

Region: Global      SW Version: Avaya BCM50 Release 6

Manufacturing SW version: 50.06

**Feature licenses**

Status	Name	Data	Expiry Date
ACTIVE	ICC	1	
ACTIVE	UM seat	2	
ACTIVE	Fax Suite	1	
ACTIVE	VPIM/AMIS	1	
ACTIVE	Q.SIG	1	
ACTIVE	MCDN	1	
ACTIVE	LANCTE Seat	2	
ACTIVE	VoIP GW T...	8	
ACTIVE	IP Client s...	4	
ACTIVE	Int Digital ...	12	

Load Keycode File...

6. If you prompted to reboot the BCM after entering the keycode file select the **Administration** tab followed by **Utilities**, **Reboot** and then click the **Reboot** button.

**Task Navigation Panel**

Configuration **Administration**

- General
- System Metrics
- Telephony Metrics
- Utilities
  - BCM Monitor
  - Ping
  - Trace Route
  - Ethernet Activity
  - Reboot**
  - Reset
  - Diagnostic Settings
  - IP Set Port Details
  - LAN IP Capture
- Backup and Restore
- Logs
- Auto-Administration Manager
- Software Management

**Reboot**

Reboot | Scheduled Reboot

**This will temporarily stop all services**

Reboot

**This action stops all services in preparation for shutdown**

Shutdown System

**Note:** The feature status change in the keycodes panel may take up to one minute to display depending on the system load and component response. You can refresh the keycode window to see the feature status change, after adding the keycode file, by selecting the refresh button in Element Manager. Some keycodes require the BCM to be rebooted.

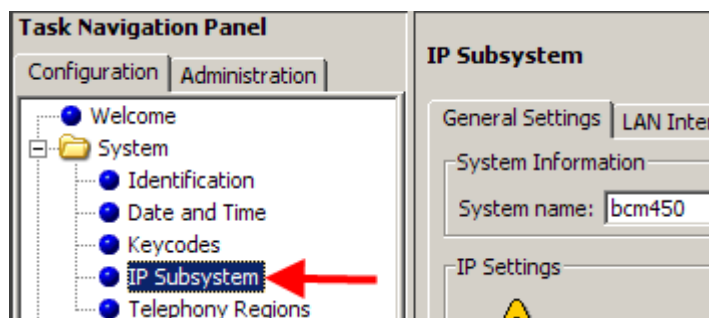
## Configuring the LAN IP Address

If the IP Address of the BCM system requires changing, i.e. to suit the customer's network, use the following procedure.

**Note:** If configuring a BCM50(b)e, you must ensure that the Router LAN IP Address and the BCM LAN IP address are on the same subnet. Refer to the **BCM50 Router LAN Settings** guide for more information.

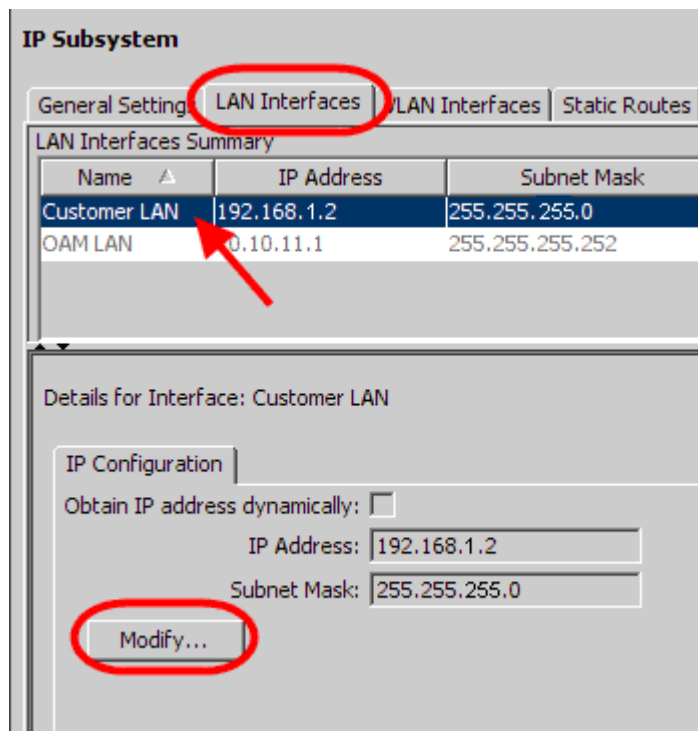
All LAN ports will use this IP Address, unless VLANs are to be configured (refer to the **VLANs Guide** for more information). The LAN IP Address does not apply to the OAM port.

1. Access Element Manager (refer to **Element Manager Connection to the BCM** section of this guide).
2. In the **Configuration** tab open the **System** heading and click on **IP Subsystem**.

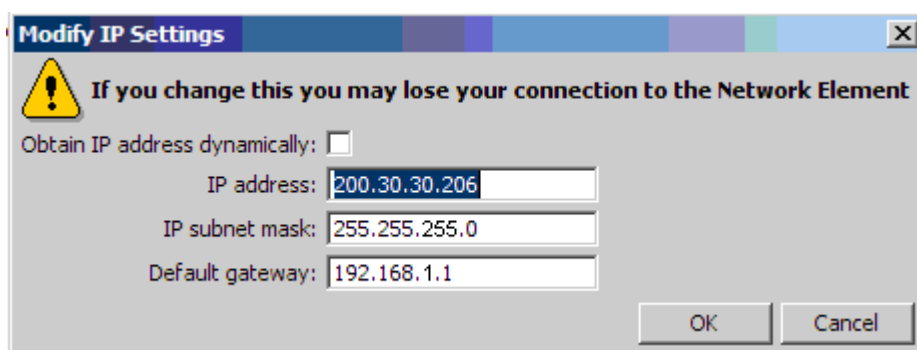




- Click on the **LAN Interfaces** tab. Select the **Customer LAN** row, and click **Modify** in the lower part of the screen.

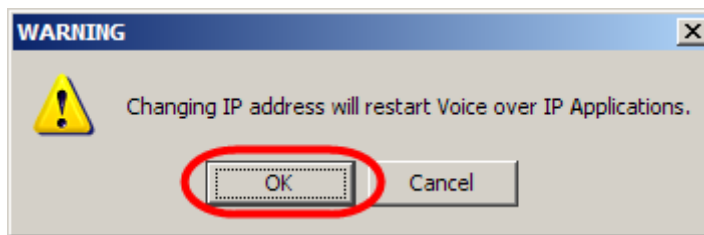


- Enter the IP Settings as required. You can choose to:
  - Obtain an IP Address, Subnet Mask, and Default Gateway automatically (refer to the **DHCP Guide** for more information on BCM and DHCP).
  - Enter an IP Address, Subnet Mask and Default Gateway manually.

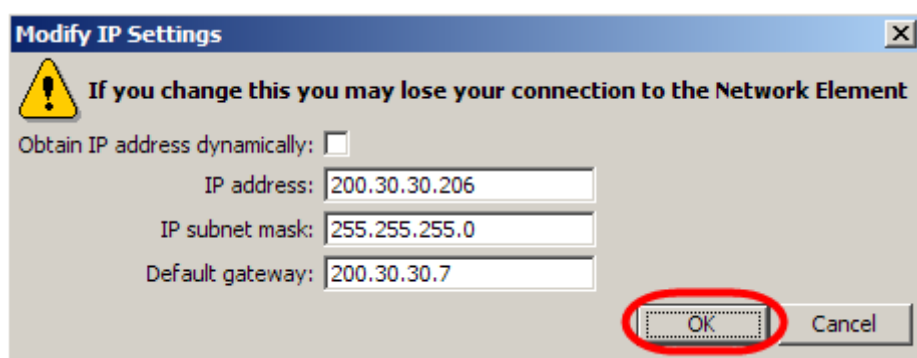


**Note:** If there is an existing DHCP server on the network, it is recommended that you specify a static IP Address for the BCM. See the network administrator about obtaining a static IP Address. Obtaining an IP Address automatically should generally only be selected when the BCM is acting as the DHCP Server for the network. Alternatively, consult the network administrator about reserving an IP Address for the BCM on their DHCP server.

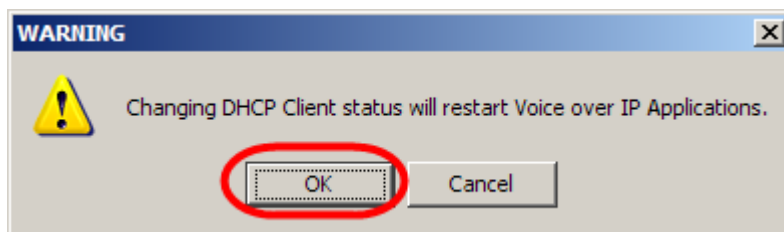
5. If you enter an IP Address manually, you will see the following WARNING box before you can configure the remaining fields. Click **OK**.



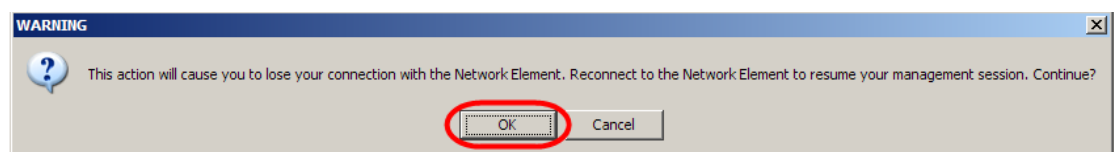
6. For manual configuration, continue entering the settings in the other fields, and click **OK**.



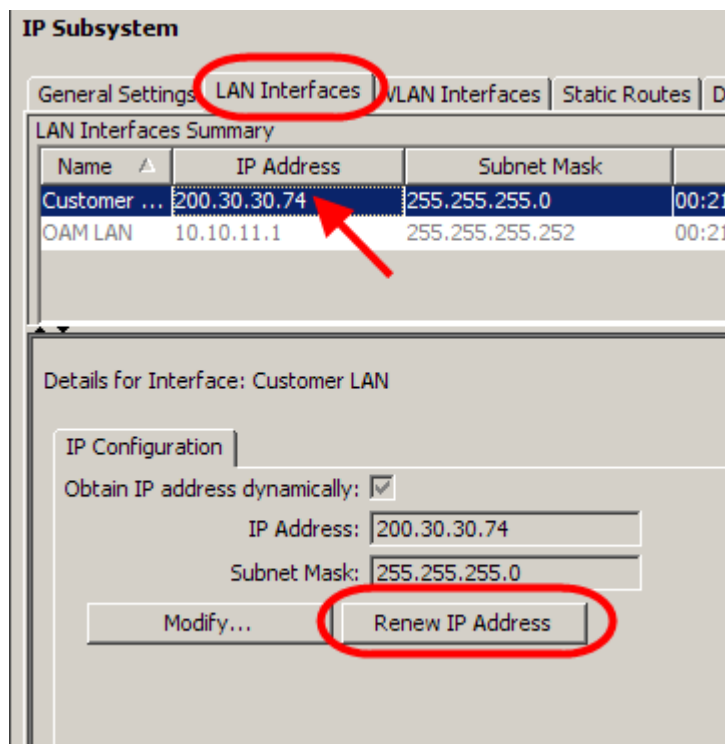
7. If Obtaining an IP Address dynamically, tick the **Obtain IP address dynamically** box. You will see the following WARNING box.



8. Click **OK** in the WARNING box, and click **OK** again in the **Modify IP Settings** box.
9. You may lose your connection to Element Manager. You will not need to reboot the BCM. Click the **OK** button, and reconnect to the BCM using the new IP address (unless connected via the OAM port).



10. If the BCM is obtaining its network settings via DHCP (either its own DHCP server or one that resides on the network), you can choose to renew the network settings. To do so, click **Renew IP Address**.



11. DNS settings can also be entered, if you are not receiving this information via DHCP. In the **IP Subsystem** area, click on the **General Settings** tab, and enter the relevant DNS information in the **DNS Settings** fields.

**IP Subsystem**

General Settings | LAN Interfaces | VLAN Interfaces | Static Routes | Dial-

System Information

System name: bcm50

IP Settings

Default gateway: 200.30.30.7

Published IP Interface: Customer LAN

Published IP Address: 200.30.30.77

Public Network

Discovered Public Address: 0.0.0.0

Address Discovery Flag: ☐

Provisioned Public Address:

Modify...

**DNS Settings**

DNS domain name: gateway.2wire.net

Primary DNS address: 192.168.1.254

Secondary DNS address:

## Configuring DHCP

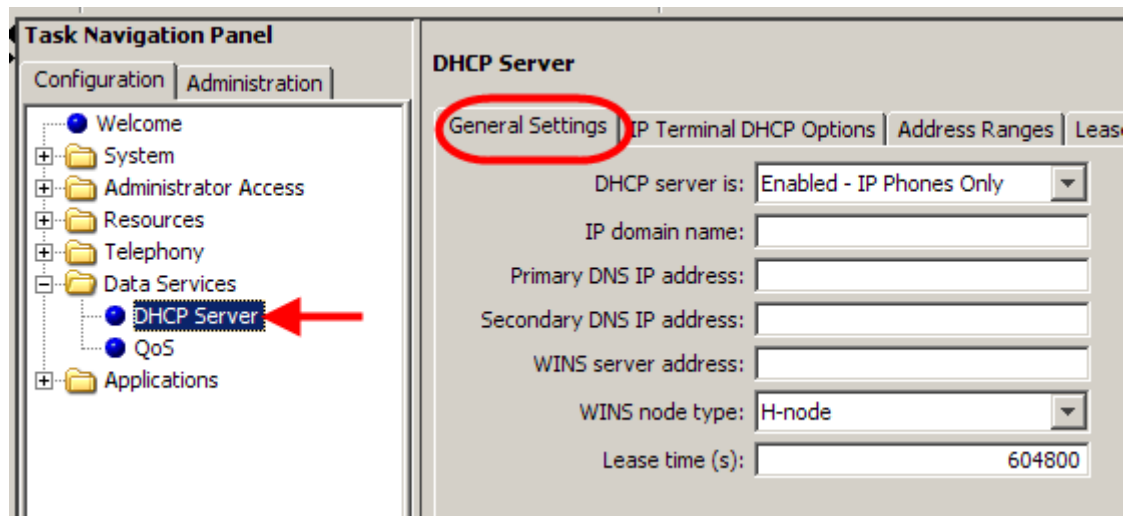
The BCM can be used as the main DHCP server for the network, or it can be used to provide DHCP information to IP Sets only. Alternatively, DHCP can be disabled on the BCM if DHCP requirements are being provided by another device on the network.

**Note:** The settings detailed in this section do not relate to DHCP on the BCM50(b)e routers. For information on the BCM50(b)e DHCP settings, refer to the **BCM50 Router LAN Settings Guide**.

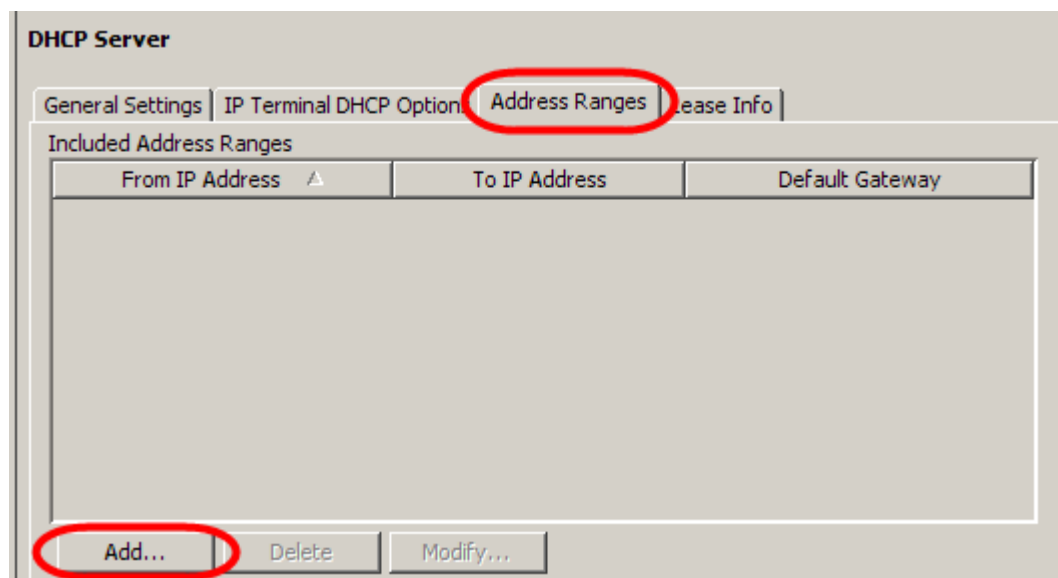
**Note:** On the BCM50(b)e models, it is possible to choose between using the DHCP service on the main DHCP unit, or the DHCP service on the router. If the router card DHCP service is used, the main module DHCP service is automatically disabled.

**Note:** For full instructions on configuring DHCP on the standard BCM50 model, or if using the core DHCP service on the main module rather than the BCM50(b)e router, refer to the **DHCP Guide**.

1. From the **Configuration** tab, open the **Data Services** folder, and select **DHCP Server**.
2. Select the **General Settings** tab. It is normally selected by default.



3. Configure the DHCP server attributes as required.
4. The BCM does not automatically create an address range of IP Addresses for allocation to DHCP clients. If the BCM is to be configured as a DHCP server (for IP Phones only or all devices) you will need to create an address range. Click on the **Address Ranges** tab.



5. Click on the **Add** button. Enter the following settings and click **OK**:
  - From IP Address: Start of the range of IP Addresses to be issued to DHCP clients
  - To IP Address: End of the range of IP Addresses to be issued to DHCP clients.
  - Default Gateway: Gateway address for this range to use.

6. This range will be issued to DHCP clients, if the BCM is configured to be a DHCP server.

**Note:** For full details concerning the registration and configuration of IP Phones, refer to the *IP Telephony Guide*.

## General Settings Screen Settings

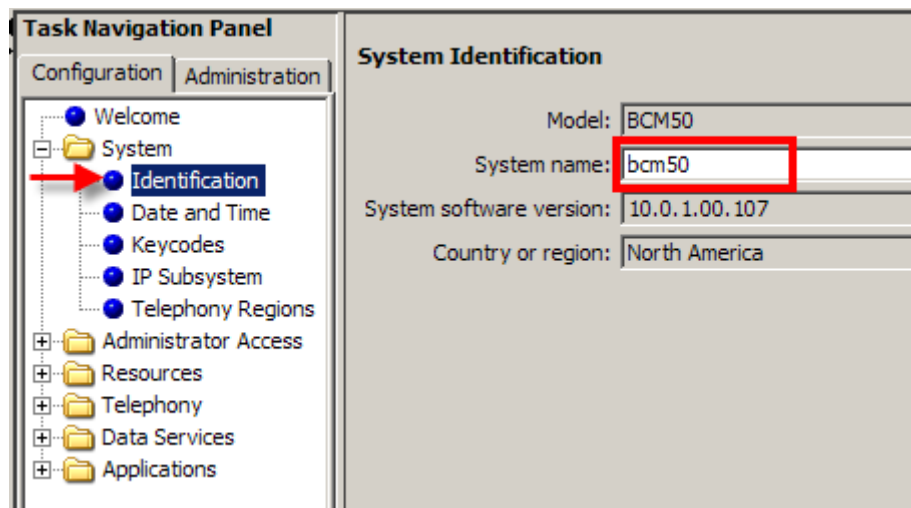
Attribute	Value	Description
The DHCP Server is	Disabled Enabled - IP Phones Only Enabled - All Devices	Determines the functionality of the DHCP server. Default: Enabled – IP Phones Only
IP domain name	<alphanumeric character string>	The domain name of the network.
Primary DNS IP address	<IP Address, format 10.10.10.10>	The IP address of the primary DNS to be used by DHCP clients.
Secondary DNS IP address	<IP Address, format 10.10.10.10>	The IP address of the secondary DNS to be used by DHCP clients.
WINS server address	<IP Address, format 10.10.10.10>	The address of the Windows Internet Server, which resolves IP addresses on a DHCP network.
WINS node type	<drop-down menu>	The type of WINS node: <ul style="list-style-type: none"> <li>• B-node: The BCM first checks the HMHOSTS cache, then uses broadcast for name registration and resolution.</li> <li>• P-node: The BCM registers with a NetBIOS Name server at startup.</li> <li>• M-node: Mixes B- and P-node. The BCM uses the B-node method, and if that fails, uses the P-node method.</li> <li>• H-node: Uses both B- and P-node methods. B-</li> </ul>

Attribute	Value	Description
		node is used only as a last resort. Default: H-node
Lease time(s)	<numeric string>	The amount of time before a DHCP lease expires and the device must request a new IP address. Default: 604800 seconds

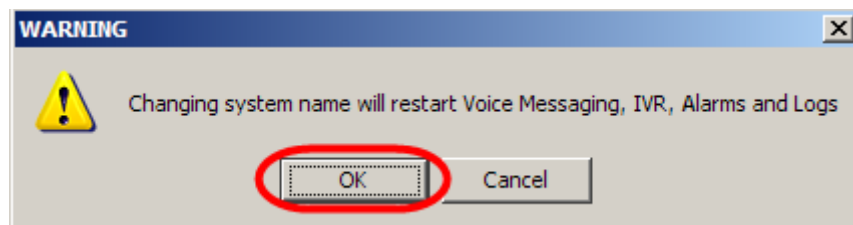
## Setting the System Name

This name is used for identification purposes.

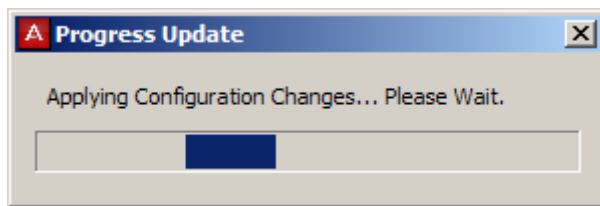
1. From the **Configuration** tab, open the **System** folder to expand it.
2. Select **Identification** from the **System** folder.
3. Enter a name for your system in the **System name** field, and press the tab key.



4. A dialog box will appear advising you of any system interruptions. Click **OK** to continue.

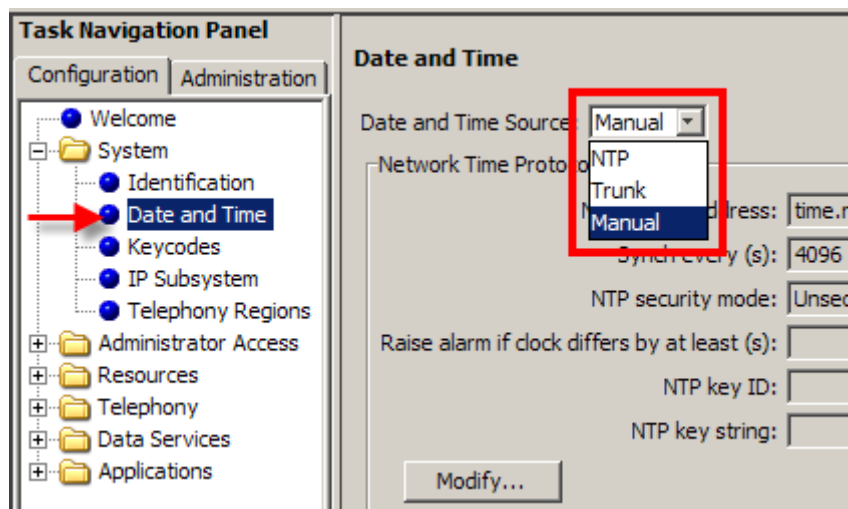


5. A Progress Update window will appear.



## Setting the Date and Time

1. From the **Configuration** tab, open the **System** folder to expand it.
2. Select **Date and Time** from the **System** folder. The **Date and Time** panel displays.



3. Select the appropriate **Date and Time Source**.



- If setting the Date and Time Source as **NTP**, click on the **Modify** button.

**Date and Time**

Date and Time Source: Manual

Network Time Protocol Settings

NTP server address: time.nist.gov

Synch every (s): 4096

NTP security mode: Unsecured

Raise alarm if clock differs by at least (s): 10

NTP key ID: 0

NTP key string:

Modify...

- Configure the NTP settings as required, and click **OK**.

**Modify Network Time Protocol Settings**

NTP server address: time.nist.gov

Synch every (s): 4096

NTP security mode: Unsecured

Raise alarm if clock differs by at least (s): 10

NTP key ID: 0

NTP key string:

OK Cancel

- If setting the Date and Time Source as **Manual**, click on the **Date and Time** drop down arrow, and use the control to select the correct date and time. Click **OK** when finished.

**Current Date and Time**

Date and time: 2010-08-16 15:34:35

Time zone: August 2010

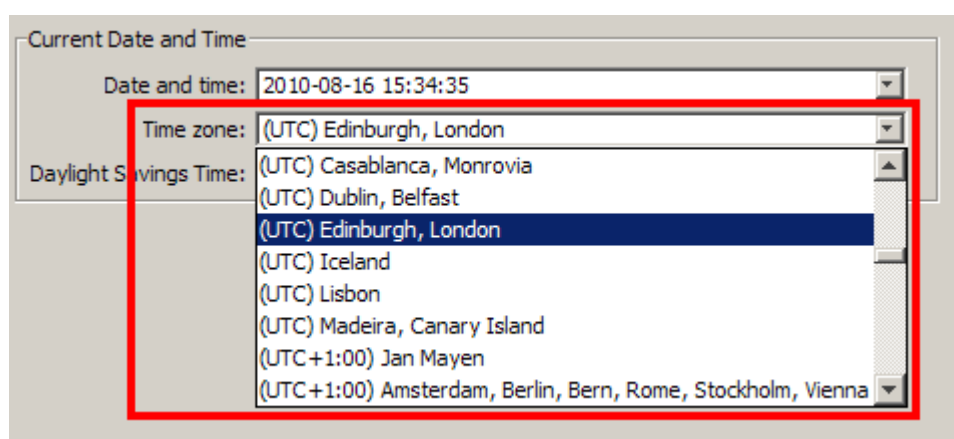
Daylight Savings Time:

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Time: 3 34 35 PM

OK Cancel

- Also ensure that the correct **Time Zone** is selected.



## Date & Time Settings

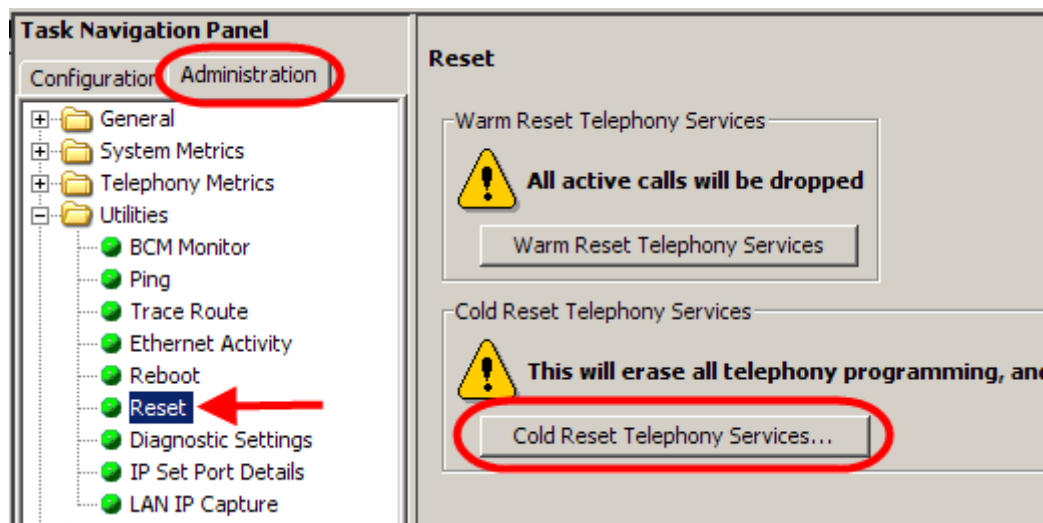
Attribute	Description
Date and Time Source	NTP: Set to NTP (Network Time Protocol) if the system uses a network server to determine the correct time and date. Trunk: Set to Trunk to use time and date settings from a CO through an analog or IDSN line. Manual: Set to Manual if you want to be able to manually configure the time and date for your system. Default: Manual
NTP server address	If Date and Time Source is set to NTP, then enter an address for the server.
Synch every (s)	The number of seconds between synchronization with the NTP server.
NTP security mode	Select whether the NTP security mode is secured or unsecured.
Raise alarm if clock differs by at least (s)	The number of discrepancy seconds specified that must occur before the system notifies you of a time difference between the BCM time and the NTP server, if the system automatically checks with the NTP server.
NTP key ID	ID for accessing the NTP server.
NTP key string	Control key corresponding to ID for accessing the NTP server
Date and time	Use the dropdown calendar to select the correct date and time.
Time zone	Select the time zone for this system.

## Setting the Start DN and Telephony Region

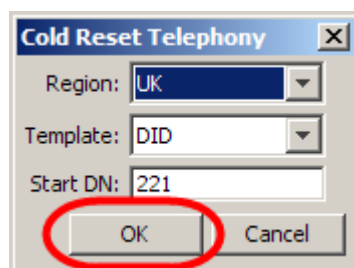
Use the following procedure to set your first extension number, telephony template, and telephony region.

- From the **Administration** tab, double-click the **Utilities** folder to expand it.
- Select **Reset** from the Utilities folder.

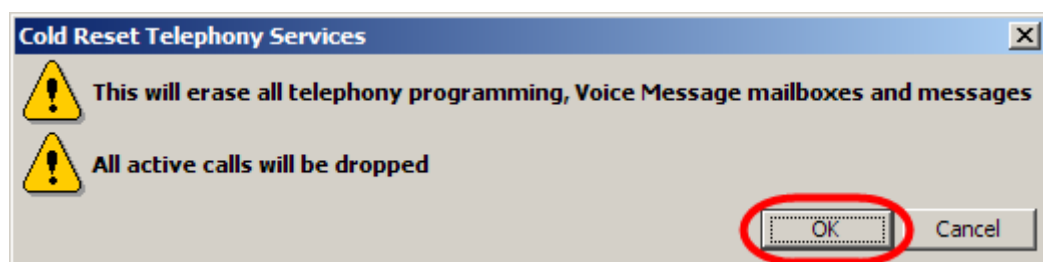
3. Click **Cold Reset Telephony Services**.



4. The Cold Reset Telephony dialog box displays. Configure the Telephony **Region**, **Template**, and **Start DN** and click **OK**.



5. A dialog box will appear advising you of service interruptions. Read the warnings and click **OK**.

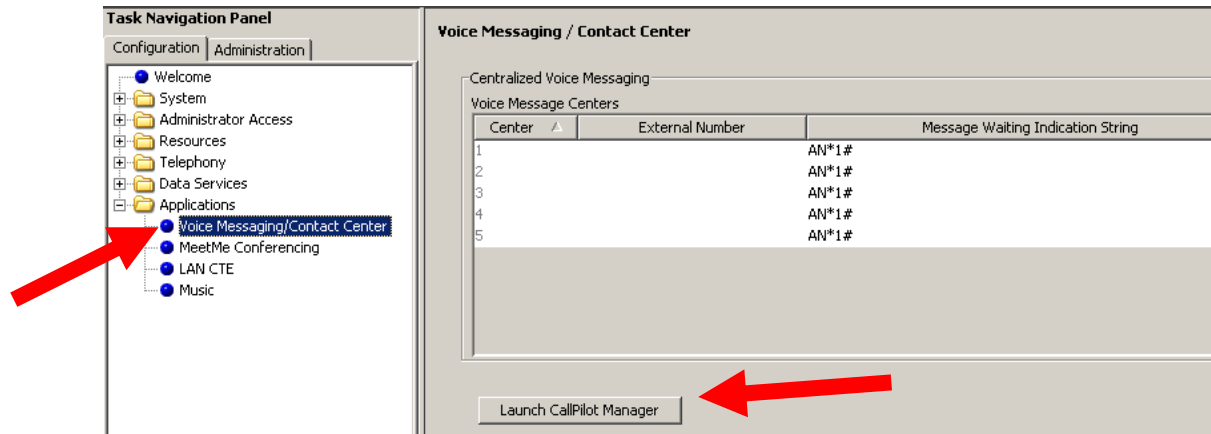


6. The reset will take a few minutes to perform. It is advisable that you do not perform any programming until the Cold Reset is complete.

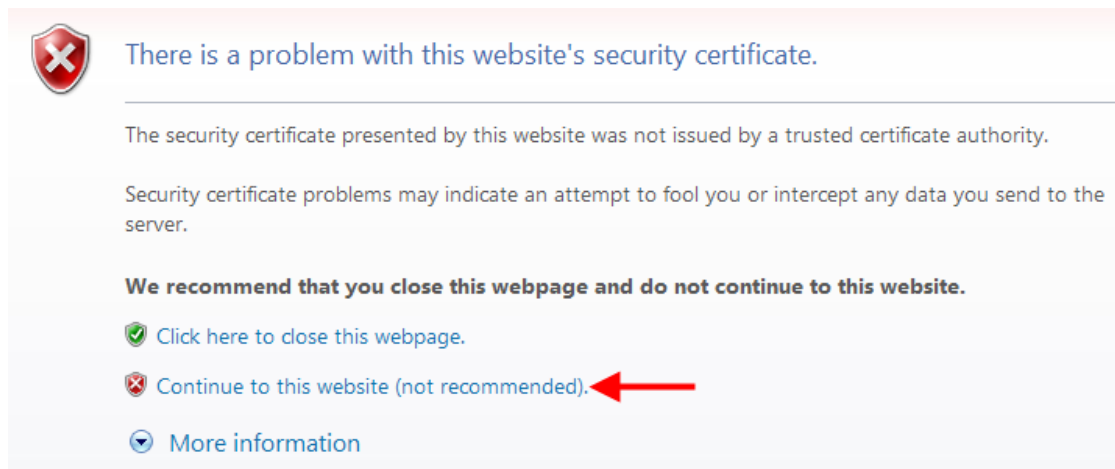
## Initialising CallPilot Manager

Use the following procedure to initialise the CallPilot Voice Messaging system.

1. From the **Configuration** tab, open the **Applications** folder.
2. Select **Voice Messaging/Contact Center** from the Applications folder.



3. Click **Launch CallPilot Manager**. If you see the below screen, click on **Continue to this website (not recommended)**.



- The Quick Install Wizard form displays. If your VoiceMail system is already initialized, you will not see the Quick Install Wizard.

## Quick Install Wizard

Please provide values for the following system settings:

Attendant DN:

Primary UI Style:

Primary Language:

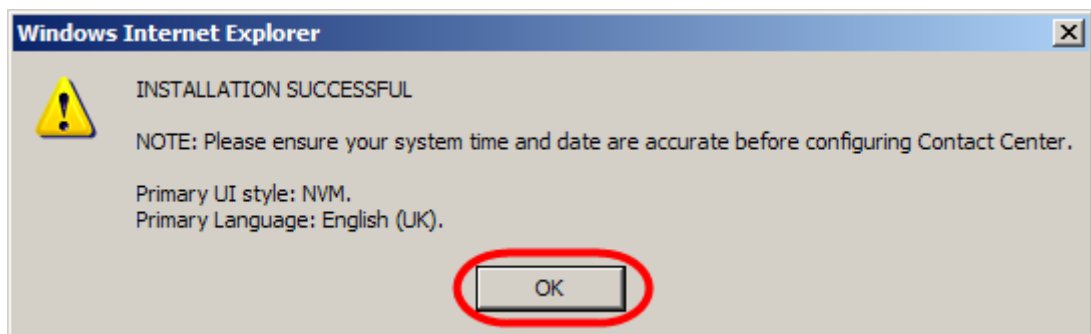
Identify the range of lines to be answered by auto-attendant:

From Line:

To Line:

Number of rings:

- Configure the attributes on the **Quick Install Wizard** form and click **Install**.
- You will see the INSTALLATION SUCCESSFUL box. Click **OK** to close this.



### Quick Install Wizard Settings

Attribute	Description
Attendant DN	Enter the extension number of the attendant or operator assigned to CallPilot.
Primary UI Style	Select the mailbox user interface used as a default for the mailboxes. If you select NVM, the mailbox user interface uses Norstar Voice Mail voice and text prompts. If you select CallPilot, the mailbox user interface uses CallPilot voice and text prompts.
Primary Language	Select the language used as the primary language for the mailboxes.

Attribute	Description
From Line	Enter the line number of the first line in the range of lines you want CallPilot to answer. CallPilot answers the range of lines between this line and the line you enter in the To Line box.
To Line	Enter the line number of the last line in the range of lines you want CallPilot to answer.
Number of rings	Enter the number of rings you want CallPilot to wait before answering lines.

## Media Bay Modules

Media Bay Modules can be defined in two main categories:

- Trunk Media Bay Modules
- Station Media Bay Modules

There are also specialised modules that, for example, provide a combination of both lines and extensions.

### Media Bay Module Configuration

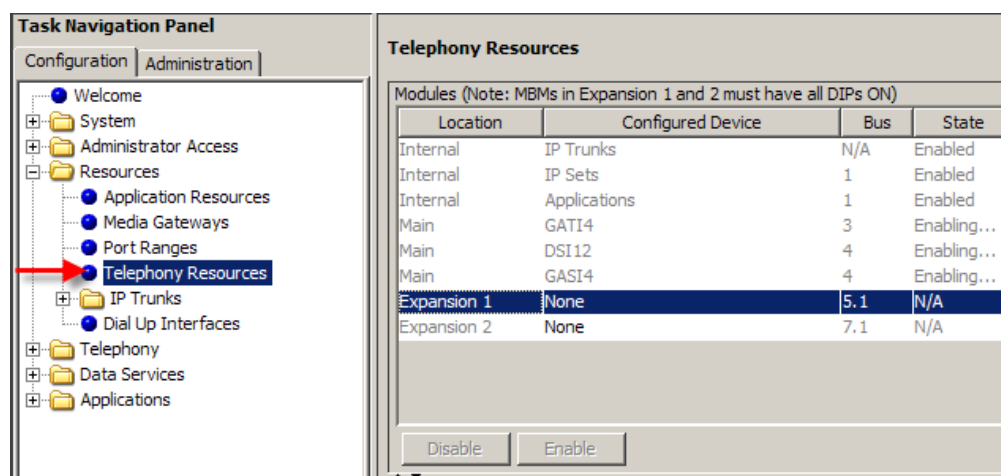
All configurations in this section are performed in Element Manager Configuration.

**Note:** Keycodes are required for the Expansion Ports to function. Ensure these have been entered (refer to the **Software Keycodes** section of this guide).

When the Media Bay Modules are configured, the status lights will stop flashing.

### Configuring the Media Bay Modules

1. In Element Manager Configuration tab, open the **Resources** heading, and click on **Telephony Resources**.



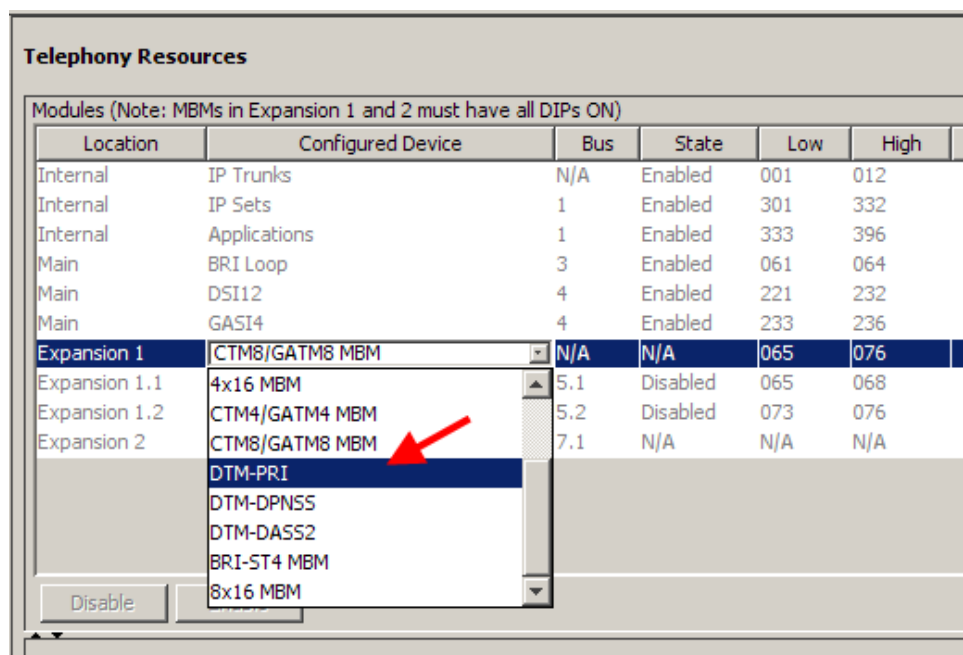
2. You can now proceed with configuring the Media Bay Module type.

### **Trunk Media Bay Modules**

Media Bay Module	Utility
DTM Digital (Trunk Media Bay Module)	Connects digital public switched telephone lines to the BCM system (PRI, DASS2, DPNSS)
CTM4/CTM8 (Caller ID Media Bay Module)	Connects a maximum of four (CTM4) or eight (CTM8) analog public switched telephone lines to the BCM system.
ISDN BRI Module ( Basic Rate Interface)	Connects a maximum of four ISDN BRI S/T interfaces.
GATM4/GATM8 (Global Analogue Trunk Module)	Connects 4/8 analog public switched telephone lines to the BCM system.
ADID4/ADID8	Connects 4/8 Analog Direct Inward Dial trunks to the system.

### **PRI Modules**

1. Double click the **Module Type** and select **DTM- PRI** from the drop down list. Press the tab key on your keyboard to enforce the change.



- In this example the system has a single PRI Digital Trunk Media Bay Module installed and the clock source has been set to Primary External to reflect this. The protocol should also be set as required. In this example Euro has been selected (other options are SL-1 and QSIG).

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State	Low
Internal	IP Trunks	N/A	Enabled	001
Internal	IP Sets	1	Enabled	301
Internal	Applications	1	Enabled	333
Main	BRI Loop	3	Enabled	061
Main	DSI12	4	Enabled	221
Main	GASI4	4	Enabled	233
Expansion 1	DTM-PRI	5.1	Disabled	065
Expansion 2	None	7.1	N/A	N/A

Disable **Enable**

Details for Module: Expansion 1 DTM-PRI

Trunk Module Parameters | Trunk Port Details | Provision Lines

Trunk type: PRI Overlap receiving: ☐

Protocol: Euro

Clock source: Secondary external

## Clock Sources and Digital Trunk Modules

For each DTM and BRI, choose one of the following settings: **Primary external**, **Secondary external**, or **Internal**:

- Primary external:** The DTM/BRI obtains the timing from the network and the system synchronizes to it. This is the default value for the first DTM in a BCM. **Private network:** If this system is in a private network and is intended to provide the master clock for that private network, the system must have one, and only one, Primary clock reference on a DTM or BRI. If this system is intended to act as clock master in a private network, then all clock sources should be set to Timing Master on this system.
- Secondary external:** The DTM/BRI acts as a standby reference point. If there are excessive errors on the Primary reference link, or the DTM/BRI designated as Primary reference fails, the Secondary DTM/BRI obtains the timing from the network to be used for system synchronization. This is the default value for the second DTM in a BCM. **Private network:** If this system is in a private network and is intended to provide the Master clock for that private network, then there



should be no Secondary reference defined on any DTM/BRI. Note that there should only be one defined Secondary clock source on a system.

- **Internal:** The DTM/BRI does not obtain timing from the network, but transmits the internally-generated system timing, from the Primary/Secondary source, to equipment to which it is connected. Note that while in the absence of a DTM Primary clocking source a BRI module can be used for the primary timing reference, it is always recommended that, when possible, DTM(s) be used as primary (and secondary) clock sources and that any remaining DTMs/BRIs be set to Timing Master.
3. The module type has been set. Any module specific settings will be displayed in the lower window. Note that Line numbers will be displayed in the **Low** and **High** fields for the module.

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State	Low	High	Active	B
Internal	IP Trunks	N/A	Enabled	001	012		12
Internal	IP Sets	1	Enabled	301	332		0
Internal	Applications	1	Enabled	333	396		23
Main	BRI Loop	3	Enabled	061	064		4
Main	DSI12	4	Enabled	221	232		2
Main	GASI4	4	Enabled	233	236		4
Expansion 1	DTM-PRI	5.1	Disabled	065	094		0
Expansion 2	None	7.1	N/A	N/A	N/A		N/A

Disable Enable

Details for Module: Expansion 1 DTM-PRI

Trunk Module Parameters | Trunk Port Details | Provision Lines

Trunk type: PRI

Protocol: Euro

Clock source: Secondary external

Overlap receiving: ☐

E1 Parameters

CRC4: ☒

4. As a general rule for Trunk modules (PRI, BRI, DASS2 etc.) you may wish to check that the lines/loops are provisioned. If the lines/loops are de-provisioned, the BCM will not have access to those lines/loops.

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus
Internal	IP Trunks	N/A
Internal	IP Sets	1
Internal	Applications	1
Main	BRI Loop	3
Main	DSI12	4
Main	GASI4	4
Expansion 1	DTM-PRI	5.1
Expansion 2	None	7.1

Disable Enable

Details for Module: Expansion 1 DTM-PRI

Trunk Module Parameters Trunk Port Details **Provision Lines**

Line	Provisioned
065	<input checked="" type="checkbox"/>
066	<input checked="" type="checkbox"/>
067	<input checked="" type="checkbox"/>
068	<input checked="" type="checkbox"/>
069	<input checked="" type="checkbox"/>
070	<input checked="" type="checkbox"/>

5. The module should now be **Enabled**.

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus
Internal	IP Trunks	N/A
Internal	IP Sets	1
Internal	Applications	1
Main	BRI Loop	3
Main	DSI12	4
Main	GASI4	4
Expansion 1	DTM-PRI	5.1
Expansion 2	None	7.1

Disable **Enable**

Details for Module: Expansion 1 DTM-PRI

Trunk Module Parameters Trunk Port Details Provision Lines

## PRI Module-Specific Settings

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State	Low	High	Active
Internal	IP Trunks	N/A	Enabled	001	012	12
Internal	IP Sets	1	Enabled	301	332	0
Internal	Applications	1	Enabled	333	396	23
Main	BRI Loop	3	Enabled	061	064	4
Main	DSI12	4	Enabled	221	232	2
Main	GASI4	4	Enabled	233	236	4
Expansion 1	DTM-PRI	5.1	Disabled	065	094	0
Expansion 2	None	7.1	N/A	N/A	N/A	N/A

Disable Enable

Details for Module: Expansion 1 DTM-PRI

Trunk Module Parameters Trunk Port Details Provision Lines

Trunk type: PRI Overlap receiving: ☐

Protocol: Euro E1 Parameters CRC4: ☒

Clock source: Secondary external

Attribute	Value	Module/line type									
Trunk type		All trunks									
	Indicates the type of trunks. This field is read-only for all modules except DTM modules.										
Trunk mode	DS/CLID, Global, Legacy	Loop									
	<ul style="list-style-type: none"><li>DS/CLID: displays for old North American LS/DS or CLID analog trunk modules, the old analog MBM, or the GATM with North American DIP switch settings.</li><li>Global: displays for the GATM MBM with no regional DIP switches set.</li><li>Legacy: displays for all other (old) analog trunk modules</li></ul>										
Protocol	NI-2, DMS-100, DMS-250, AT&T4ESS, SL-1, Euro, ETSI Q.Sig					PRI					
	Choose the trunk protocol used by your service provider. The supported protocols are: PRI-T1: NI (NI-1 and NI-2), DMS-100, DMS-250, AT&T4ESS, SL-1 PRI-E1: ETSI QSIG, Euro, SL-1 Note: SL-1 and ETSI QSIG require an MCDN keycode to display. BRI: Protocol can also be selected on BRI T-loops under the Configuration > Resources > Telephony Resources. <b>Note:</b> Always check the line protocol with the central office.										
NSF Extension	None, WATS, ALL					PRI					
	The Network Specific Facilities (NSF) information element is used to request a particular service from the network. Settings are based on the type of switch to which the line connects. Suggested settings: DMS-100/250: NONE Siemens ESWD, Lucent 5ESS: WATS GTD5, DMS-10: ALL When you select NONE, the NSF extension bit is not set for any service. When you select WATS, the NSF extension bit is set for unbanded OUTWATS calls. When you select ALL, the NSF extension is always set for all CbC services.										

Attribute	Value	Module/line type									
	Appears only for NI protocol.										
Protocol type	User, Network					PRI					
	When you select SL-1 protocol, an additional setting, Protocol type, appears. SL-1 protocol is a private networking protocol. This allows you to designate a BCM node as a Network (controller). The default setting is User (client). In public network configurations, the CO is generally considered the Network side or controller. Applies to SL-1 protocol only.										
B-channel selection sequence	Ascending Sequential Descending Sequential					PRI					
	Defines how B-channel resources are selected for call processing.										
Answer timer	1, 2, 3, 4, or 5 sec.		E&M			PRI					
	Set the minimum duration of an answer signal before a call is considered to be answered.										
Disconnect timer	60, 100, 260, 460, or 600 milliseconds	Loop			T1						
	Specify the duration of an Open Switch Interval (OSI) before a call on a supervised external line is considered disconnected. This setting must match the setting for the line at the central office (CO). You must enable disconnect supervision by changing the Line <b>Trunk mode</b> attribute. Under the Telephony Services sub-heading, choose Lines and Line/trunk Data.										
Clock Source	Primary External Secondary External Internal				T1	PRI	*BRI S/T			DASS2	
	Designates whether the DTM/BRI acts as a primary or secondary timing component for an external timing source or as the internal timing source. <b>Note:</b> A BRI module can be programmed with primary/secondary clock source, however, it is recommended that a BRI module always be set to Internal if a DTM exists on the system to be the Primary External clock source. <b>Warning: Changing the clock source may disconnect calls.</b> If you change the clock source for your system, you may cause your system DTM interface(s) to reset, resulting in dropped calls. Choose a suitable time to change the clock source and use the Page feature to inform users of possible service disruptions.										
Send Name Display	Select or clear					PRI	*BRI QSIG				
	When you select this check box, the system sends a specified outgoing name display (OLI) from the calling telephone. Appears only for Protocols: SL-1, NI, DMS-100, DMS-250, or PRI QSIG.										
Remote Capability MWI	Select or clear					PRI					
	This setting allows you to indicate MWI compatibility on the specific loop(s) that you are using to connect to the central voice mail system on a Meridian 1 which has the MWI package installed, with the RCAP setting set to MWI. Appears only for SL-1 protocol.										
Overlap receiving							BRI				
	Supports target lines in markets which use Overlap receiving signalling on the BRI trunks. Overlap receiving must be configured for each BRI loop. After every digit is received at the ISDN layer, Target Lines are checked for matches. If a full match is made, the call is routed immediately to the target line without waiting for additional digits.										
Local Number Length							BRI				
	When Overlap receiving is enabled on the trunks, this number determines how many incoming digits need to match the target line numbers to be considered a call for that target line.										
Host node	M1, Embark, IDPX, DSM										DPNSS
	DPNSS cards connected to Embark switches have a different way of handling call diversion, therefore, when you provision a DTM for DPNSS, you must indicate what type of switch the lines are connected to. When you select the Embark switch, calls are diverted using the Call Forwarding feature instead of call diversion.										
Local											DPNSS

Attribute	Value	Module/line type										
Number Length	This number allows the system to determine how many digits to read on an incoming call to determine that the call is meant for this system.											
Maximum Transits	Default: 31					PRI						
	Indicate the maximum number of times that a call will be transferred within the SL-1 network before the call is dropped. Protocol must be set to SL-1 to display this field.											
T1 parameters												
CO fail					T1	PRI						
	Specify a carrier failure standard (T1A-5474, TR62411)											
Interface levels	ISDN, PSTN				T1	PRI						
	Define a loss plan setting.											
Framing	ESF, SF				T1	PRI						
	Select the framing format used by your T1 or PRI service provider: Extended Superframe (ESF) or Superframe (SF). Contact your T1 or PRI service provider for the proper setting. (SF or Superframe is sometimes known as D4.)											
Line coding	B8ZS, AMI				T1	PRI						
	Define the encoding signals on a T1 line. Select the standard used by your T1 service provider. Contact your T1 service provider for the proper setting.											
Internal CSU	<check box>				T1	PRI						
	Turn the internal T1 channel service unit (CSU) on or off.											
CSU line build	0, 7.5, or 15 dB				T1	PRI						
	Set the gain level of the transmitted signal. This setting appears only when the Internal CSU is Enabled.											
DSX1 build	000-100, 100-200, 200-300, 300-400, 400-500, 500-600, or 600-700 feet				T1	PRI						
	Set the distance between BCM and an external channel service unit. This setting only appears when the Internal CSU is Disabled. Contact your service provider for the proper settings.											
CRC4	<check box>					E1 PRI						
	Ensure this is enabled or disabled to match the service provider Cyclic Redundancy Check (CRC4) setting for the trunk.											

## DASS2 Modules

1. Double click in the **Configured Device** field and set it to **DTM – DASS2** module.

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State	Low
Internal	IP Trunks	N/A	Enabled	001
Internal	IP Sets	1	Enabled	301
Internal	Applications	1	Enabled	333
Main	BRI Loop	3	Enabled	061
Main	DSI12	4	Enabled	221
Main	IASI4	4	Enabled	233
Expansion 1	DTM-DASS2	5.1	Disabled	065
Expansion 2	None	7.1	N/A	N/A

Details for Module: Expansion 1 DTM-DASS2

Trunk Module Parameters | Trunk Port Details | Provision Lines

Trunk type:

Clock source:

2. Configure the options as required.

## DASS2 Module-Specific Settings

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State	Low	High
Internal	IP Trunks	N/A	Enabled	001	012
Internal	IP Sets	1	Enabled	301	332
Internal	Applications	1	Enabled	333	396
Main	BRI Loop	3	Enabled	061	064
Main	DSI12	4	Enabled	221	232
Main	GASI4	4	Enabled	233	236
Expansion 1	DTM-DASS2	5.1	Disabled	065	094
Expansion 2	None	7.1	N/A	N/A	N/A

Disable Enable


Details for Module: Expansion 1 DTM-DASS2

Trunk Module Parameters | Trunk Port Details | Provision Lines

Trunk type: DASS2

Clock source: Secondary external

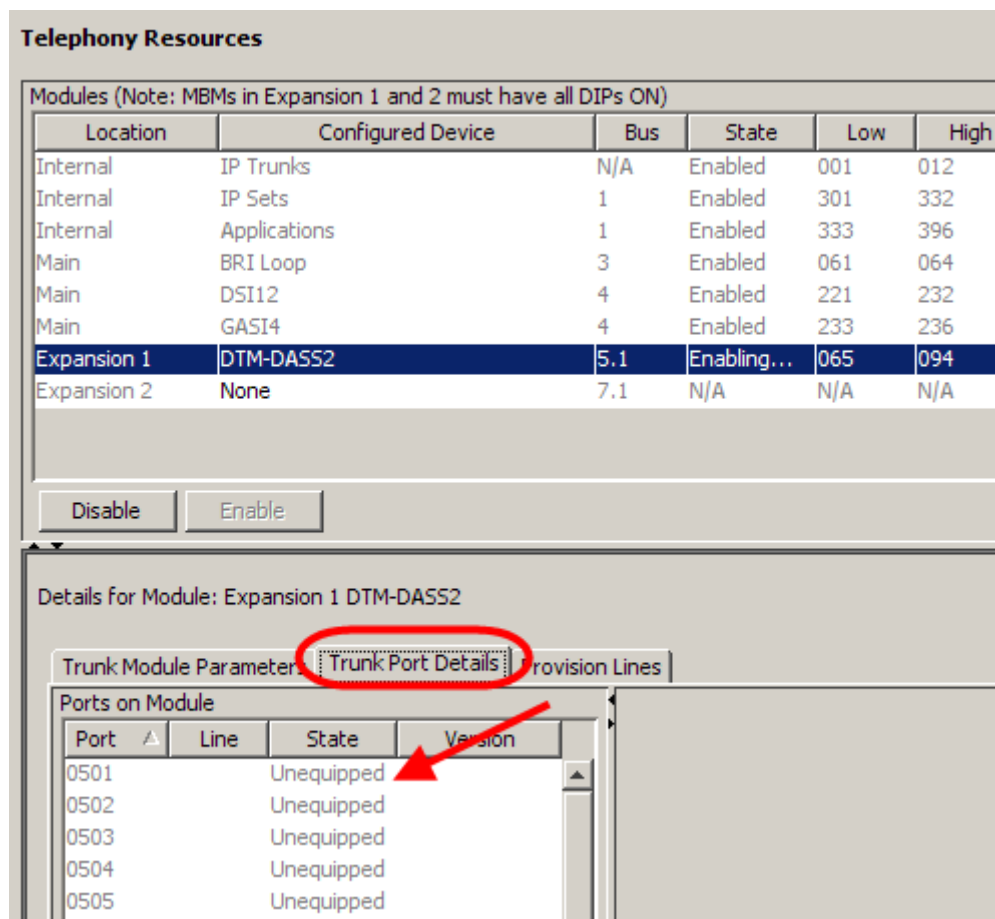
Primary external  
Secondary external  
Internal



Attribute	Value	Module / Line Type						
Clock Source	Primary	External	T1	PRI	*BRI S/T	*BRI U2	*BRI U4	DASS2
	Secondary	External						
	Internal							
	<p>Designates whether the DTM/BRI acts as a primary or secondary timing component for an external timing source or as the internal timing source.</p> <p><b>Note:</b> A BRI module can be programmed with primary/secondary clock source, however, it is recommended that a BRI module always be set to Internal if a DTM exists on the system to be the Primary External clock source.</p> <p><b>Warning: Changing the clock source may disconnect calls.</b> If you change the clock source for your system, you may cause your system DTM interface(s) to reset, resulting in dropped calls. Choose a suitable time to change the clock source and use the Page feature to inform users of possible service disruptions.</p>							

## Trunk Port Details tab

- Both trunk and analog station modules show port details. Ports settings are directly related to the physical ports into which the PSTN lines or telephony devices connect on the media bay modules.



Attribute	Value	Module type							
Port #	Read-only	All modules							
	<ul style="list-style-type: none"><li>These are the port numbers of the physical device.</li></ul>								
Device type	Read-only	All modules							
	<ul style="list-style-type: none"><li>This is the type of module.</li></ul>								
Line #	00X-XXX	CTM/GATM4	CTM/GATM8	Combo	DTM-T1	DTM-PRI	BRI-T		
	The number of lines depends on the module type.								
Call State or State	Idle Active Deprovisioned	All modules							
	This field indicates whether a module line or DN is in use or even provisioned.								
Version	<read-only>	All modules							
	This field indicates the version of firmware running on the module.								
DN	XXXX							ASM/GASM	DSM
	Each port supports one telephone, hence, one DN record.								
Addons		All modules							



Attribute	Value	Module type
	Indicates auxiliary items added to the telephony devices or trunks	
	Add-on	This is a list number.
	Type	This field indicates the type of add-on, such as a KIM module.
	Version	This field indicates the version of firmware running on the add-on device.

- Open the **Provision Lines** tab and check that the required lines are provisioned by clicking each line, and change the setting if necessary.

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State	Low	High
Internal	IP Trunks	N/A	Enabled	001	012
Internal	IP Sets	1	Enabled	301	332
Internal	Applications	1	Enabled	333	396
Main	BRI Loop	3	Enabled	061	064
Main	DSI12	4	Enabled	221	232
Main	GAS14	4	Enabled	233	236
Expansion 1	DTM-DASS2	5.1	Disabled	065	094
Expansion 2	None	7.1	N/A	N/A	N/A

Disable Enable

Details for Module: Expansion 1 DTM-DASS2

Trunk Module Parameters Trunk Port Details **Provision Lines**

Lines

Line	Provisioned
065	<input checked="" type="checkbox"/>
066	<input checked="" type="checkbox"/>
067	<input checked="" type="checkbox"/>
068	<input checked="" type="checkbox"/>
069	<input checked="" type="checkbox"/>
070	<input checked="" type="checkbox"/>

- The module should now be **Enabled**.

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State	Low
Internal	IP Trunks	N/A	Enabled	001
Internal	IP Sets	1	Enabled	301
Internal	Applications	1	Enabled	333
Main	BRI Loop	3	Enabled	061
Main	DSI12	4	Enabled	221
Main	GAS14	4	Enabled	233
Expansion 1	DTM-DASS2	5.1	Disabled	065
Expansion 2	None	7.1	N/A	N/A

Disable **Enable**

Details for Module: Expansion 1 DTM-DASS2

## DPNSS Modules

1. Double click in the **Configured Device** field and set to **DTM - DPNSS** module.

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State	Low	High
Internal	IP Trunks	N/A	Enabled	001	012
Internal	IP Sets	1	Enabled	301	332
Internal	Applications	1	Enabled	333	396
Main	BRI Loop	3	Enabled	061	064
Main	DSI12	4	Enabled	221	232
Main	IASI4	4	Enabled	233	236
Expansion 1	DTM-DASS2	5.1	Disabled	065	094
Expansion 2	4x16 MBM	7.1	N/A	N/A	N/A
	CTM4/GATM4 MBM				
	CTM8/GATM8 MBM				
	DTM-PRI				
	DTM-DPNSS				
	DTM-DASS2				
	BRI-ST4 MBM				
	8x16 MBM				

Disable

Details for Module:

Trunk Module Parameters | Trunk Port Details | Provision Lines

Lines

Line	Provisioned
065	<input checked="" type="checkbox"/>
066	<input checked="" type="checkbox"/>
067	<input checked="" type="checkbox"/>
068	<input checked="" type="checkbox"/>
069	<input checked="" type="checkbox"/>
070	<input checked="" type="checkbox"/>

2. From the **Host Node** option list, select the node type that the BCM is connected to.

Main	IASI4	4	Enabled	233	236
Expansion 1	DTM-DPNSS	5.1	Disabled	065	094
Expansion 2	None	7.1	N/A	N/A	N/A

Disable Enable

Details for Module: Expansion 1 DTM-DPNSS

Trunk Module Parameters | Trunk Port Details | Provision Lines | Provision Virtual Channels

Trunk type: DPNSS

Clock source: Secondary external

Host node: M1

DPNSS local number length

Maximum transits

M1  
Embark  
ISDX  
DMS

3. Configure the other options as required

## DPNSS Module-Specific Settings

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State	Low	High	Active
Internal	IP Trunks	N/A	Enabled	001	012	
Internal	IP Sets	1	Enabled	301	332	
Internal	Applications	1	Enabled	333	396	
Main	BRI Loop	3	Enabled	061	064	
Main	DSI12	4	Enabled	221	232	
Main	GASI4	4	Enabled	233	236	
Expansion 1	DTM-DPNSS	5.1	Disabled	065	094	
Expansion 2	None	7.1	N/A	N/A	N/A	

Disable Enable

**Details for Module: Expansion 1 DTM-DPNSS**

Trunk Module Parameters | Trunk Port Details | Provision Lines | Provision Virtual Channels

Trunk type:  Host node:

Clock source:  DPNSS local number length:

Maximum transits:

Attribute	Value	Description
Clock Source	Primary Secondary Timing Master	Designates whether the DTM/BRI acts as a primary or secondary timing component for an external timing source or as the internal timing source. Note: A BRI module can be programmed with primary/secondary clock source, however, it is recommended that a BRI module always be set to Internal if a DTM exists on the system to be the Primary External clock source.
Host node	M1 Embark IDPX DSM	DPNSS cards connected to Embark switches have a different way of handling call diversion, therefore, when you provision a DTM for DPNSS, you must indicate what type of switch the lines are connected to. When you select the Embark switch, calls are diverted using the Call Forwarding feature instead of call diversion.
DPNSS Local Number Length	1-10	This number allows the system to determine how many digits to read on an incoming call to determine that the call is meant for this system.

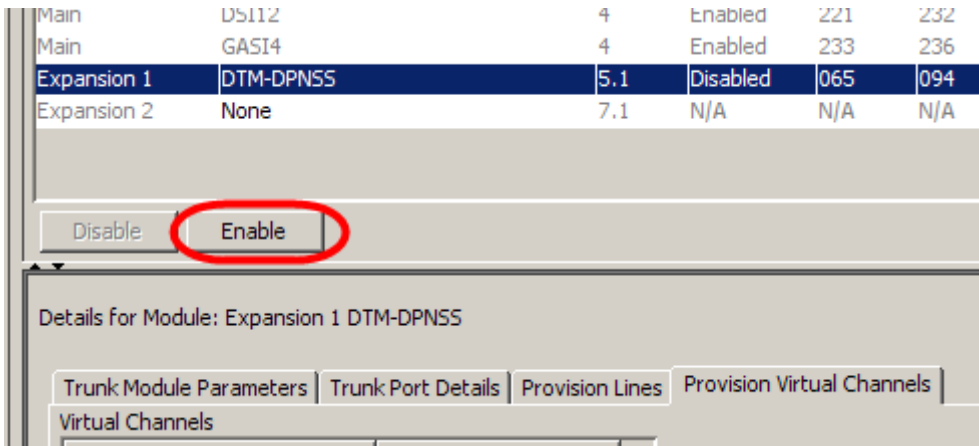
4. Open the **Provision Lines** tab and check that the required lines are provisioned by clicking each line, and change the setting if necessary.

Line	Provisioned
065	<input checked="" type="checkbox"/>
066	<input checked="" type="checkbox"/>
067	<input checked="" type="checkbox"/>
068	<input checked="" type="checkbox"/>
069	<input checked="" type="checkbox"/>
070	<input checked="" type="checkbox"/>

5. Click the **Provision Virtual Channels Tab**. A virtual channel is a channel assigned to the DPNSS module. If the check box is selected beside a channel, that channel is available for call traffic. Provision the Channels as required by checking the tick boxes.

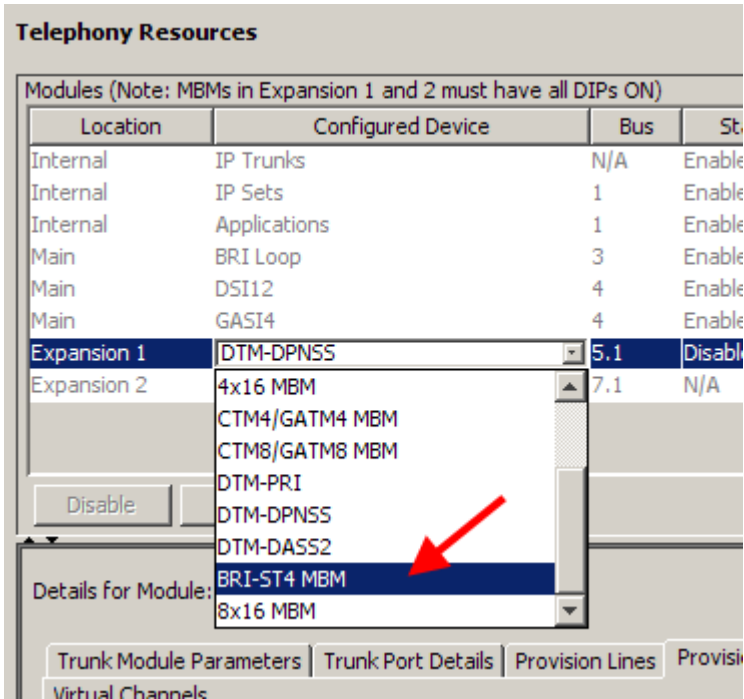
Virtual Channel	Provisioned
01	<input type="checkbox"/>
02	<input type="checkbox"/>
03	<input type="checkbox"/>
04	<input type="checkbox"/>
05	<input type="checkbox"/>
06	<input type="checkbox"/>

6. The module should be **Enabled** once configured.

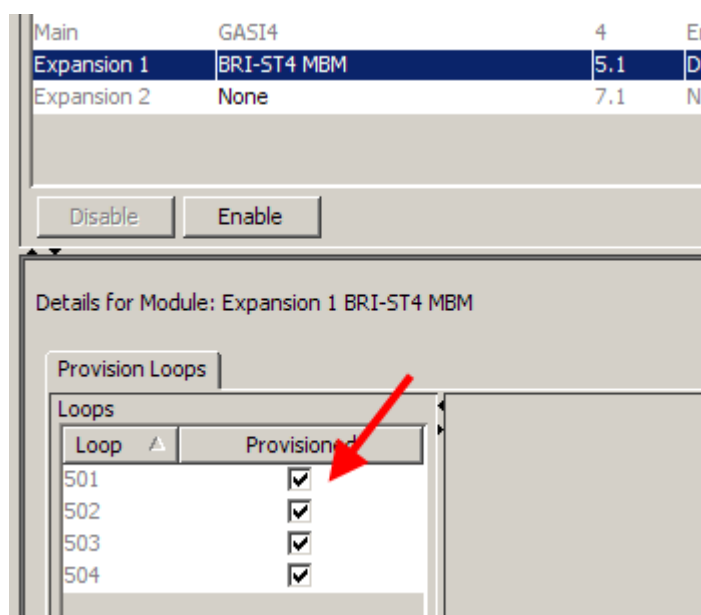


### ***BRI Module***

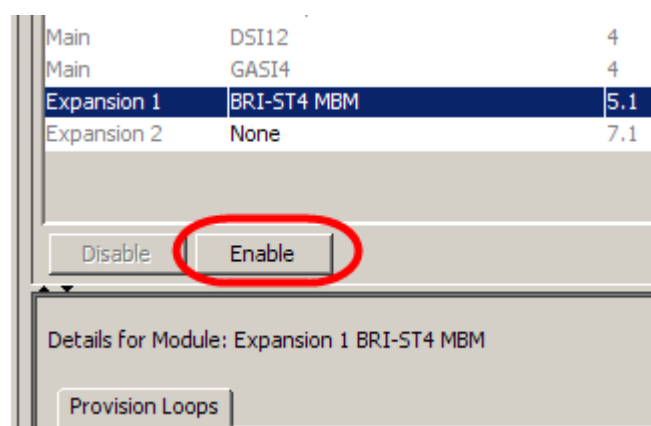
1. Double click in the **Configured Device** field and set it to **BRI-ST4 MBM**.



2. View the **Provision Loops** tab and check that the required lines are provisioned by clicking each line, and change the setting if necessary.



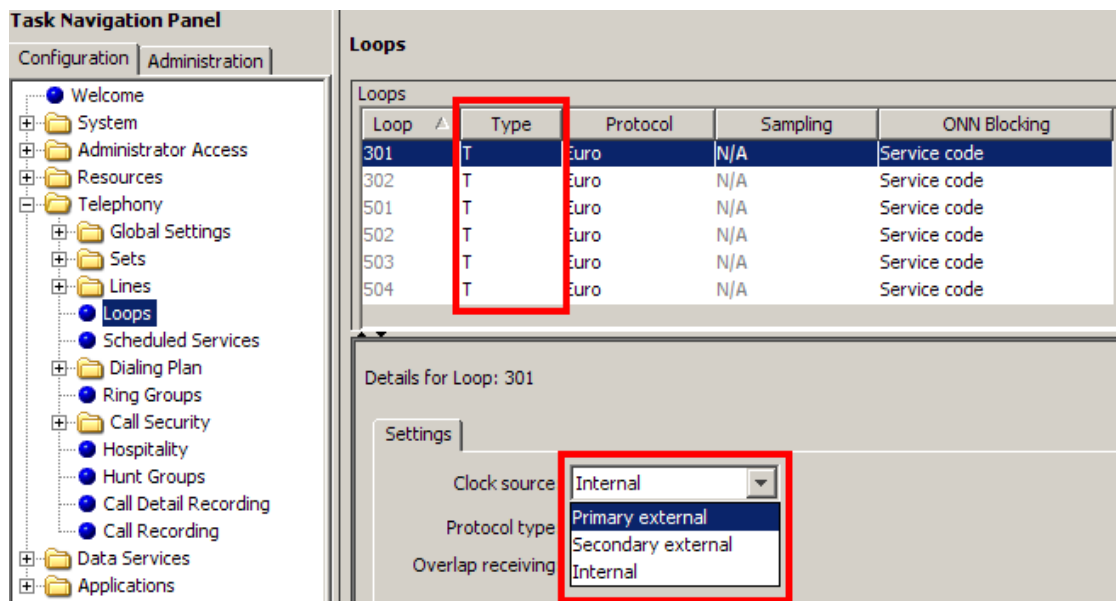
3. There are no module-specific settings for BRI modules.
4. The module should now be **Enabled**.



Use the following procedure to configure the **BRI loop type**, i.e. **S** or **T** and also the **Clock Source** settings for the BRI loops.

1. Open **Telephony**, then **Loops**.
2. Select the **Loop** to configure.

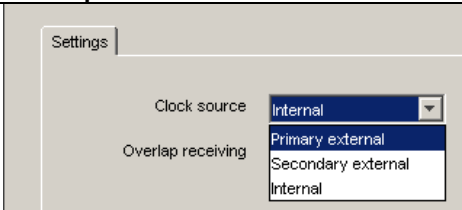
3. Select the **Loop Type** from the option box provided.



4. Configure the loops and clock source accordingly.

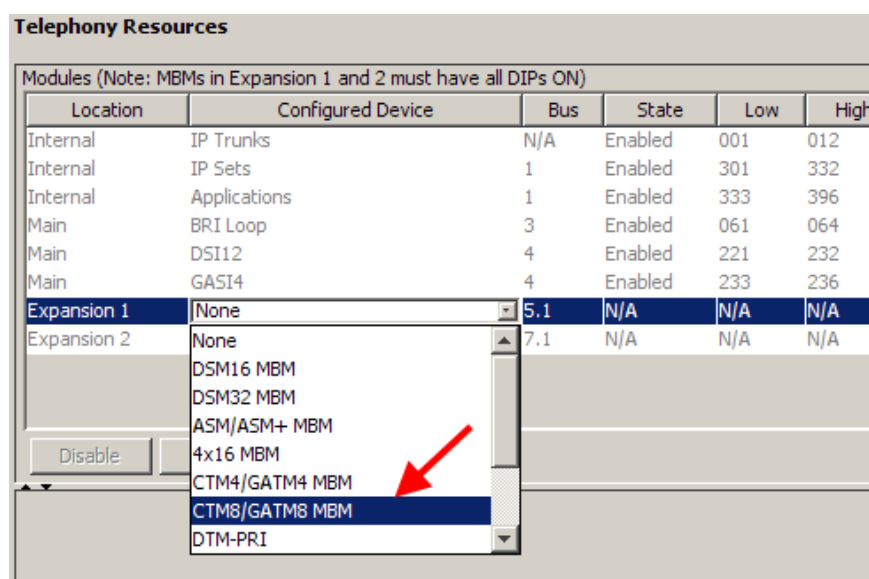
### Loop Settings

Attribute	Value	Description															
<div><div>Loops</div><div><div>Loops</div><table><tr><th>Loop</th><th>Type</th><th>Protocol</th><th>Sampling</th><th>ONN Blocking</th></tr><tr><td>501</td><td>T</td><td>Euro</td><td>N/A</td><td>Service code</td></tr><tr><td>502</td><td>T</td><td>Euro</td><td>N/A</td><td>Service code</td></tr></table></div></div>			Loop	Type	Protocol	Sampling	ONN Blocking	501	T	Euro	N/A	Service code	502	T	Euro	N/A	Service code
Loop	Type	Protocol	Sampling	ONN Blocking													
501	T	Euro	N/A	Service code													
502	T	Euro	N/A	Service code													
Loop	<X01-X04>	Each BRI module supports four loops (eight lines for T-loop programming).															
Type	T S	This setting defines whether the loop supports trunks (T-loop) or device connections (S-loop). Note: This variable may be different for different market profiles.															
Protocol	Euro QSIG NI-2	Select the appropriate ISDN protocol. The values displayed depend on both the market profile and software keycodes. Euro - ETSI ISDN standard QSIG - also an ETSI standard. Only appears if the ETSI QSIG keycode is loaded. NI-2															
Sampling (S-loops only)	Adaptive Fixed N/A	Select a sampling rate for the S-loop. Fixed: two or more S-interface devices use the loop, and the length of the loop is less than 200 m (650 ft.). Adaptive: two or more S-interface devices use the loop, and the length of the loop is greater than 200 m (650 ft.). If one device is using the loop, the length of the loop can be a maximum of 1000 m (3230 ft)															
ONN blocking	Suppression bit Service code N/A	Set the Outgoing Name and Number (ONN) Blocking. When you activate ONN, a user can press <b>FEATURE</b> 819 to block the outgoing name and number on a per call basis. Programming note: Ensure that all telephones that have this feature available are assigned valid OLI numbers. Refer to .															
ONN blocking		Suppression bit: the system flags the call to the Central Office (CO) so that the name and number is not sent to the person you call. Service code: VSC digits are dialed out before the called number to activate ONN at the central office. These codes are supplied by your service provider for the lines.															

Attribute	Value	Description
		
Attribute	Value	Description
Clock source	Primary External Secondary External Internal	Primary External - uses clock from PSTN Secondary External - used if system has more than one Loop Internal - uses clock on BCM
Overlap: receiving	<check box>	Supports target lines in markets which use Overlap receiving signaling on the BRI trunks. Overlap receiving must be configured for each BRI loop.
Overlap: length	0-10	Set the local number length for loops to interfaces that receive overlap rather than enbloc digits. This number is the total length of the called party number received. This number is used to calculate the number of leading digits that need to be removed by the system.
	<p>Note: This parameter appears only when Overlap receiving is enabled.  Example:  Public received number = 4502303  Target line received numbers = 303  Local number length = 7  Public received number length = 3  Thus the first four digits are deleted by the system.</p>	
Send Name Display (ETSI QSIG only)	<check box>	If the switch allows outgoing name display, select the check box.

## CTM/GATM (4 and 8 port) Module

1. Double click in the **Configured Device** field and set it to either **CTM8/GATM8** or **CTM4/GATM4** depending on which module is required.





- Then select Expansion 1.1 and configure the Disconnect timer settings as required. Repeat this process for Expansion 1.2 (CTM8/GATM8 only).

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State	Low	High
Internal	IP Trunks	N/A	Enabled	001	012
Internal	IP Sets	1	Enabled	301	332
Internal	Applications	1	Enabled	333	396
Main	BRI Loop	3	Enabled	061	064
Main	DSI12	4	Enabled	221	232
Main	GASI4	4	Enabled	233	236
Expansion 1	CTM8/GATM8 MBM	N/A	N/A	065	076
Expansion 1.1	CTM4/GATM4 MBM	5.1	Disabled	065	068
Expansion 1.2	CTM4/GATM4 MBM	5.2	Disabled	073	076
Expansion 2	None	7.1	N/A	N/A	N/A

Disable Enable

Details for Module: Expansion 1.1 CTM4/GATM4 MBM

Trunk Module Parameters Trunk Port Details

Trunk type: Loop

Disconnect timer: 460

### CTM/GATM (4 and 8 port) Module-Specific Settings

Attribute	Value	Description
Disconnect Timer	60-600ms	Set as advised by the CO. Specify the duration of an Open Switch Interval (OSI) before a call on a supervised external line is considered disconnected. This setting must match the setting for the line at the central office (CO). You must enable disconnect supervision by changing the Line Trunk mode attribute.

3. Once configured the bus should be **Enabled** (for the 8-port version, it will be necessary to **Enable** both Expansion 1.1 & 1.2).

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State	Low	
Internal	IP Trunks	N/A	Enabled	001	0
Internal	IP Sets	1	Enabled	301	3
Internal	Applications	1	Enabled	333	3
Main	BRI Loop	3	Enabled	061	0
Main	DSI12	4	Enabled	221	2
Main	GASI4	4	Enabled	233	2
Expansion 1	CTM8/GATM8 MBM	N/A	N/A	065	0
Expansion 1.1	CTM4/GATM4 MBM	5.1	Disabled	065	0
Expansion 1.2	CTM4/GATM4 MBM	5.2	Disabled	073	0
Expansion 2	None	7.1	N/A	N/A	N

Disable **Enable**

Details for Module: Expansion 1.1 CTM4/GATM4 MBM

Trunk Module Parameters | Trunk Port Details

Trunk type: Loop

Disconnect timer: 460

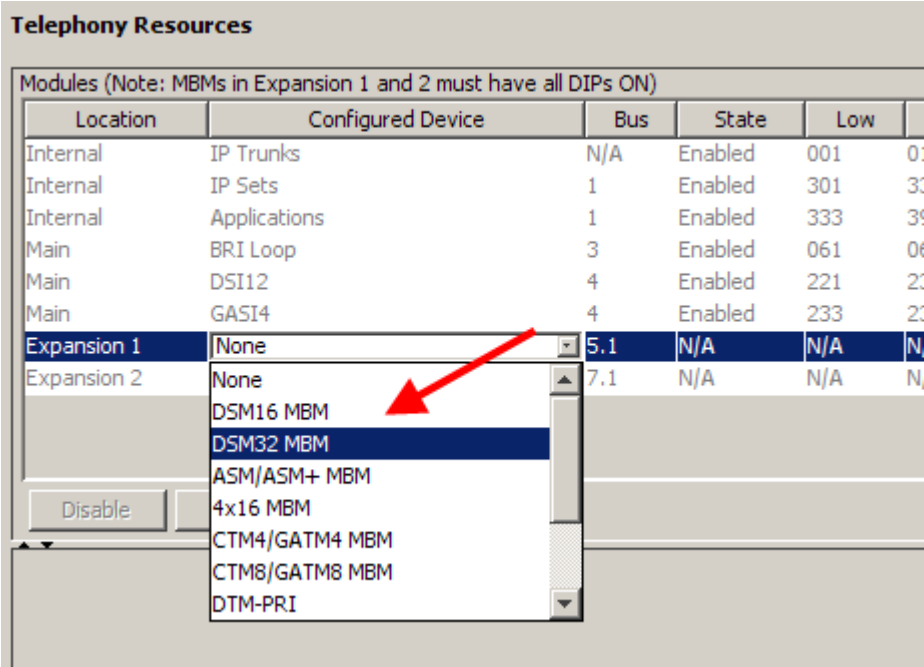
## Station Media Bay Modules

With station media bay modules (MBM) you can connect telephones and analog telecommunication devices to the BCM system.

Media Bay Module	Utility
DSM16(+)/DSM32(+) (Digital Station Module)	Connects a maximum of 16 (DSM16+) or 32 (DSM32+) digital telephones to the BCM system.
ASM4/ASM8	Connects 4/8 analog devices to the BCM system.
GASM8	Connects 4/8 analog devices to the BCM system. The GASM provides the following additional services: caller ID, pass through, message waiting indication, and disconnect supervision at the telephone. The GASM also allows you to download new firmware.

**DSM 16/32 Modules**

1. Double click in the **Configured Device** field and from the drop down list select **DSM16** or **DSM32** module.



2. Both trunk and analog modules show port details. Ports settings are directly related to the physical ports into which the PSTN lines or telephony devices connect on the media bay modules.

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State	Low
Internal	IP Trunks	N/A	Enabled	001
Internal	IP Sets	1	Enabled	301
Internal	Applications	1	Enabled	333
Main	BRI Loop	3	Enabled	061
Main	DSI12	4	Enabled	221
Main	GASI4	4	Enabled	233
Expansion 1	DSM32 MBM	N/A	N/A	237
Expansion 1.1	DSM16 MBM	5.1	Disabled	237
Expansion 1.2	DSM16 MBM	6.1	Disabled	253
Expansion 2	None	7.1	N/A	N/A

Disable Enable

Details for Module: Expansion 1.1 DSM16 MBM

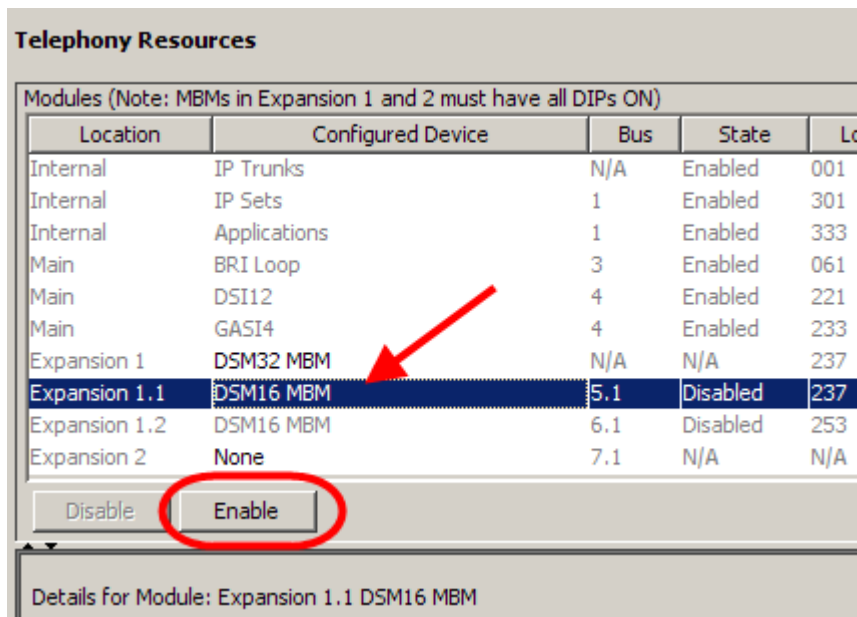
Set Port Details

Port	DN	Device type	Version	State
0501	237	Disabled by user		Disabled b...
0502	238	Disabled by user		Disabled b...
0503	239	Disabled by user		Disabled b...
0504	240	Disabled by user		Disabled b...
0505	241	Disabled by user		Disabled b...
0506	242	Disabled by user		Disabled b...
0507	243	Disabled by user		Disabled b...

## DSM16/32 Module Specific Settings

Attribute	Value	Module type
Port #	<ul style="list-style-type: none"> <li>These are the port numbers of the physical device.</li> </ul>	
Device type	Read-only	This is the type of module.
Call State or State	Idle Active Deprovisioned	<b>All modules</b>
	This field indicates whether a module line or DN is in use or even provisioned.	
Version	<read-only>	<b>All modules</b>
	This field indicates the version of firmware running on the module.	
DN	XXXX	<b>ASM/GASM</b> <b>DSM</b>
	Each port supports one telephone, hence, one DN record.	
Addons		<b>All modules</b>
	Indicates auxiliary items added to the telephony devices or trunks	
	Add-on	This is a list number.
	Type	This field indicates the type of add-on, such as a KIM module.
	Version	This field indicates the version of firmware running on the add-on device.

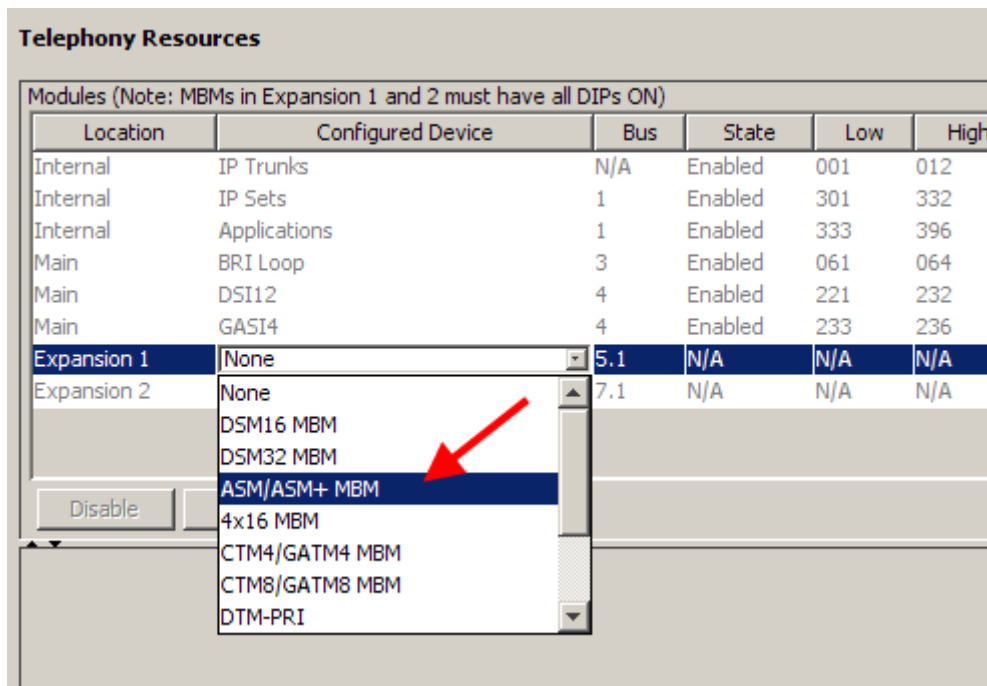
- The bus (or both busses) should now be **Enabled**.



**Note:** For the DSM32 MBM both Expansion 1.1 and Expansion 1.2 should be enabled.

## ASM Analog Station Module Configuration

- Double click in the **Configured Device** field and from the drop down list set it to **ASM/ASM+** module.



- There are no module-specific options for these modules.

3. The bus should now be **Enabled**.

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State	
Internal	IP Trunks	N/A	Enabled	00:
Internal	IP Sets	1	Enabled	30:
Internal	Applications	1	Enabled	33:
Main	BRI Loop	3	Enabled	06:
Main	DSI12	4	Enabled	22:
Main	GA5I4	4	Enabled	23:
Expansion 1	ASM/ASM+ MBM	5.1	Disabled	23:
Expansion 2	None	7.1	N/A	N/A

Disable **Enable**

## Combination Modules

These modules provide a combination of both lines and extensions.

Media Bay Modules	Utility
4x16 Combo Combination of a CTM4 and a DSM16	Connects a maximum of four analog public switched telephone lines to the BCM system. Also connects a maximum of 16 digital telephones to the BCM system.
G4/8x16	Connects 4/8 analog trunks and up to 16 digital extensions to the BCM system.

## Combination Module Configuration

1. Double click in the **Configured Device** field and select **4 or 8x16 Combo** module as required.

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State	Low	High
Internal	IP Trunks	N/A	Enabled	001	012
Internal	IP Sets	1	Enabled	301	332
Internal	Applications	1	Enabled	333	396
Main	BRI Loop	3	Enabled	061	064
Main	DSI12	4	Enabled	221	232
Main	GASI4	4	Enabled	233	236
Expansion 1	None	5.1	N/A	N/A	N/A
Expansion 2	4x16 MBM	7.1	N/A	N/A	N/A

Disable

CTM4/GATM4 MBM  
CTM8/GATM8 MBM  
DTM-PRI  
DTM-DPNSS  
DTM-DA552  
BRI-ST4 MBM  
8x16 MBM

2. Then select Expansion 1.1 (and Expansion 1.2 if the 8 x 16 MBM has been selected) and configure the Trunk Module parameters accordingly. (Please refer to the **CTM/GATM (4 and 8 port) Module** section of this guide).

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State	Low	High
Internal	IP Trunks	N/A	Enabled	001	012
Internal	IP Sets	1	Enabled	301	332
Internal	Applications	1	Enabled	333	396
Main	BRI Loop	3	Enabled	061	064
Main	DSI12	4	Enabled	221	232
Main	GASI4	4	Enabled	233	236
Expansion 1	8x16 MBM	N/A	N/A	N/A	N/A
Expansion 1.1	CTM4/GATM4 MBM	5.1	Disabled	065	068
Expansion 1.2	CTM4/GATM4 MBM	5.2	Disabled	073	076
Expansion 1.3	DSM16 MBM	6.1	Disabled	253	268
Expansion 2	None	7.1	N/A	N/A	N/A

Disable    Enable

Details for Module: Expansion 1.1 CTM4/GATM4 MBM

Trunk Module Parameters    Trunk Port Details

Trunk type: Loop

Disconnect timer: 460

- Then select Expansion 1.2 (or Expansion 1.3 if the 8 x 16 MBM has been selected) will be the DSM16 MBM.

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State	Low
Internal	IP Trunks	N/A	Enabled	001
Internal	IP Sets	1	Enabled	301
Internal	Applications	1	Enabled	333
Main	BRI Loop	3	Enabled	061
Main	DSI12	4	Enabled	221
Main	IASI4	4	Enabled	233
Expansion 1	8x16 MBM	N/A	N/A	N/A
Expansion 1.1	CTM4/GATM4 MBM	5.1	Disabled	065
Expansion 1.2	CTM4/GATM4 MBM	5.2	Disabled	073
Expansion 1.3	DSM16 MBM	6.1	Disabled	253
Expansion 2	None	7.1	N/A	N/A

Disable Enable

Details for Module: Expansion 1.3 DSM16 MBM

Set Port Details

Ports on Module

Port	DN	State
0601	253	Disabled
0602	254	Disabled
0603	255	Disabled
0604	256	Disabled
0605	257	Disabled
0606	258	Disabled

- Once configured, each bus should be **Enabled**.

**Telephony Resources**

Modules (Note: MBMs in Expansion 1 and 2 must have all DIPs ON)

Location	Configured Device	Bus	State
Internal	IP Trunks	N/A	Enabled
Internal	IP Sets	1	Enabled
Internal	Applications	1	Enabled
Main	BRI Loop	3	Enabled
Main	DSI12	4	Enabled
Main	IASI4	4	Enabled
Expansion 1	8x16 MBM	N/A	N/A
Expansion 1.1	CTM4/GATM4 MBM	5.1	Disabled
Expansion 1.2	CTM4/GATM4 MBM	5.2	Disabled
Expansion 1.3	DSM16 MBM	6.1	Disabled
Expansion 2	None	7.1	N/A

Disable **Enable**

Details for Module: Expansion 1.3 DSM16 MBM

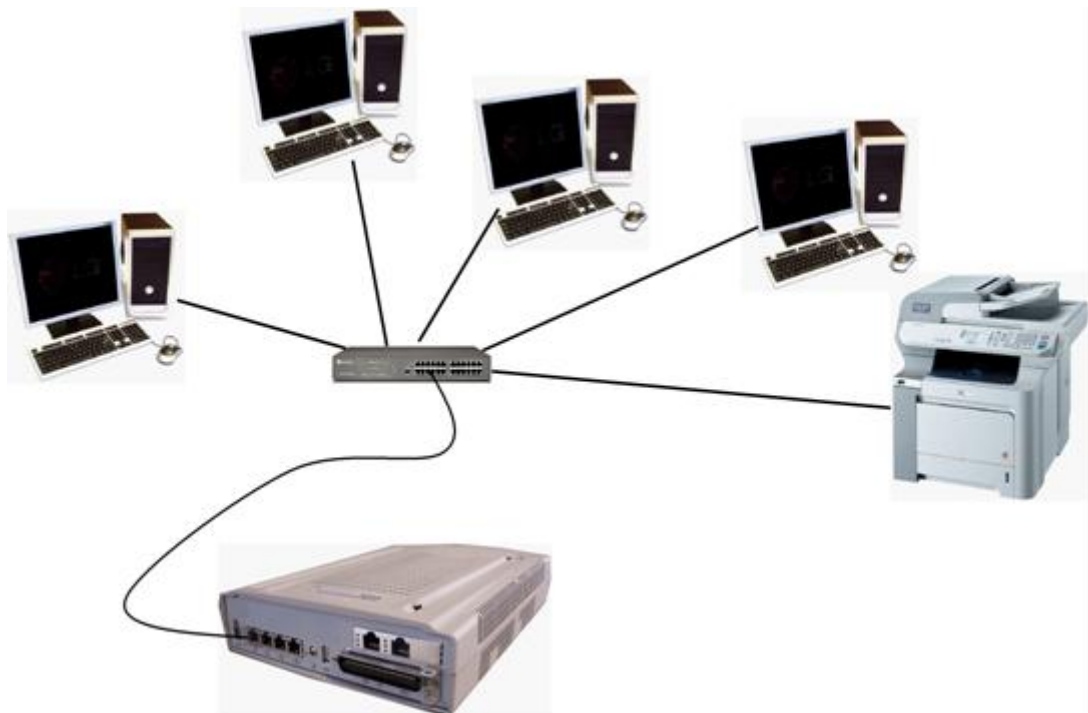


## Connecting the BCM to the Network

**NOTE:** If the BCM is in a Standalone Installation, this section should be ignored.

After the BCM has been prepared for the network, and the preceding initialisation procedures have been performed, the BCM can be connected to a Local Area Network (LAN).

1. Plug one end of a standard RJ45 patch cable into one of the LAN ports of the BCM. Plug the other end of the cable into a network connection point, e.g. a wall mounted RJ45 socket, or directly into a switch/hub.



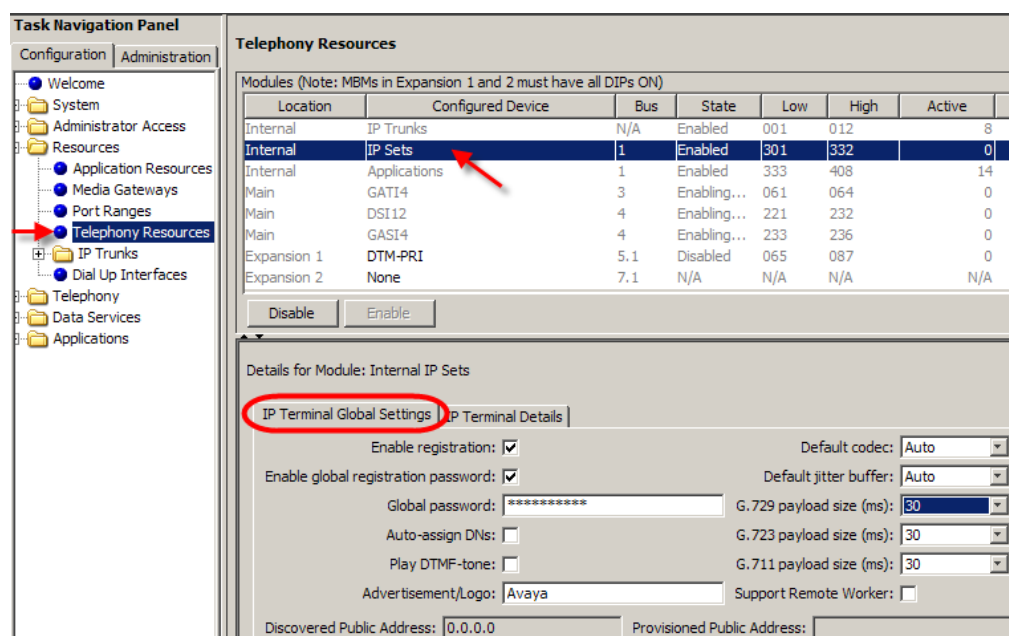
## Registering IP Terminals

The following procedure describes how to configure the BCM to allow IP Telephones to register on the BCM.

**Note:** For full instructions on how to register and set up IP terminals, including Remote worker sets, refer to the ***IP Telephony Guide***.

1. From the **Configuration** tab, open the **Resources** folder to expand it.
2. Select **Telephony Resources** from the **Resources** folder.

3. Select **IP Sets** from the **Configured Device** column. The Details for Module displays in the lower pane with the **IP Terminal Global Settings** tab as the default.
4. Configure the **IP Terminal Global Settings** attributes.



5. Now register the IP Phones.

## IP Sets – IP Terminal Global Settings

Attribute	Description
Enable registration	Set this value to ON to allow new IP clients to register with the system. <b>WARNING:</b> Remember to set Registration to Off when you have finished registering the new telephones.
Enable global registration password	If you want to require the installer to enter a password when IP telephones are configured and registered to the system, check this box. If this option is not selected, a user ID (738662) and password (266344) is requested during IP Set registration.
Global password	If the Enable Global Registration Password checkbox is selected, enter the password the installer will enter on the IP telephone to connect to the system.
Auto-assign DNs	If set to ON, the system assigns an available DN as an IP terminal requests registration. It does not prompt the installer to enter a set DN.
Advertisement logo	Any information in this field appears on the display of all IP telephones. For example, your company name or slogan.
For all other settings, please refer to the <b>IP Telephony Guide</b> .	

## Additional Information

### Startup Profile Configuration Tool

It is possible to apply Initial settings such as BCM Name, Region, IP Settings, Start DN, and a Keycode File via a Startup Profile Configuration tool. The Startup Profile Configuration tool is an **alternative** method of configuring BCM initial settings to the previous sections in this guide.

The Startup Profile is configured via an Excel spreadsheet, saved to a USB stick which is then inserted into the BCM USB port. The BCM is then powered up whereby the Startup Profile is read and the settings applied

**Note:** The Startup Profile cannot be run after the Keycodes have been applied. When the Startup Profile is successfully applied, the BCM system automatically reboots to complete the system configuration. The Startup Profile is not fully loaded until the system reboots.

**Note:** The USB storage device must be formatted for the FAT32 file system. If necessary, reformat the USB storage device by plugging it into the USB port of your computer, right-clicking the USB device icon, and selecting FAT32 reformatting. **Warning: This destroys any data you had on the USB.**

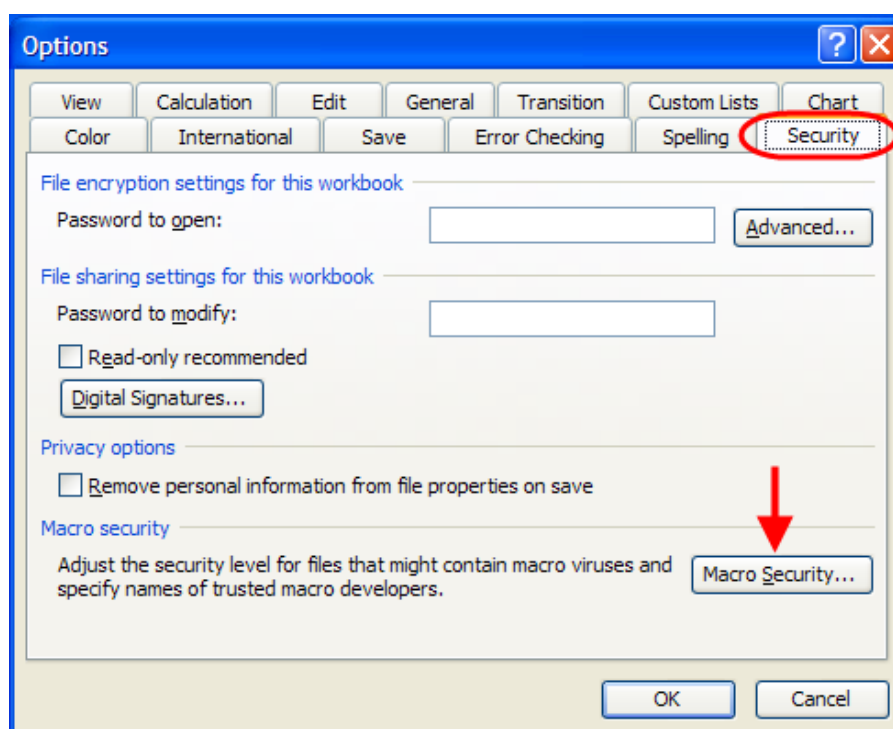
### ***Before Configuring the Startup Profile Configuration Tool***

The Startup Profile is configured via an Excel spreadsheet. In order to configure and save the Startup Profile, the Excel macros need to be disabled.

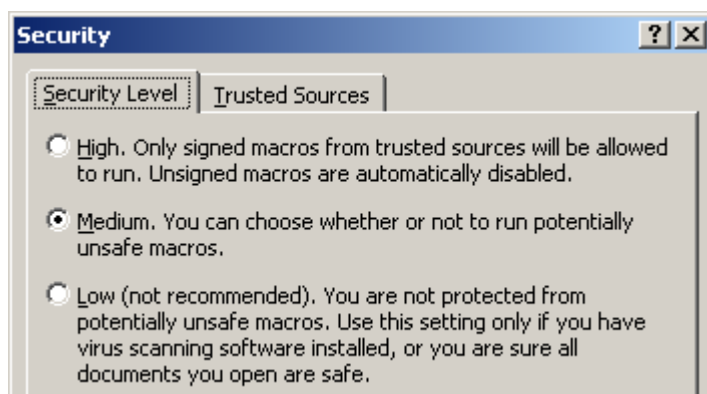
To set the Excel Macro security settings:

1. With Excel open, go to the **Tools** menu and select **Options**.
2. Select the **Security** tab.

3. Click the **Macro Security** button.



4. Select **Medium** or **Low**.



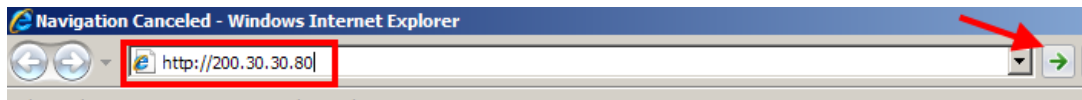
5. Click **OK** (twice).
6. Exit Excel, open the profile again, and configure as required. You can then use the large "Save" button at the top of the spreadsheet.

## Obtaining the Startup Profile Configuration Tool

The Startup Profile Configuration tool can be obtained from the BCM web page.

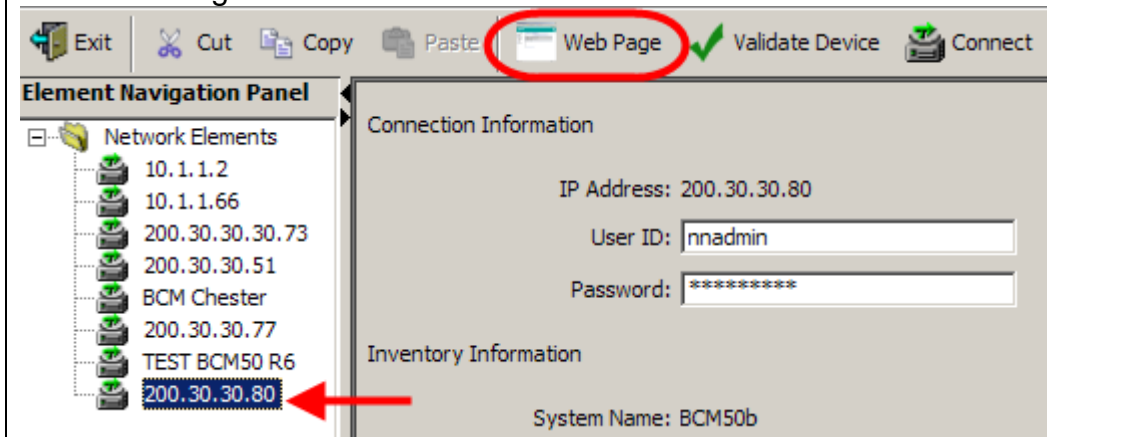
To obtain the Startup Profile Configuration tool from the BCM web page:

1. Open Internet Explorer. In the address field type (replacing the relevant part with your BCM IP address): **http://<bcm ip address>/**

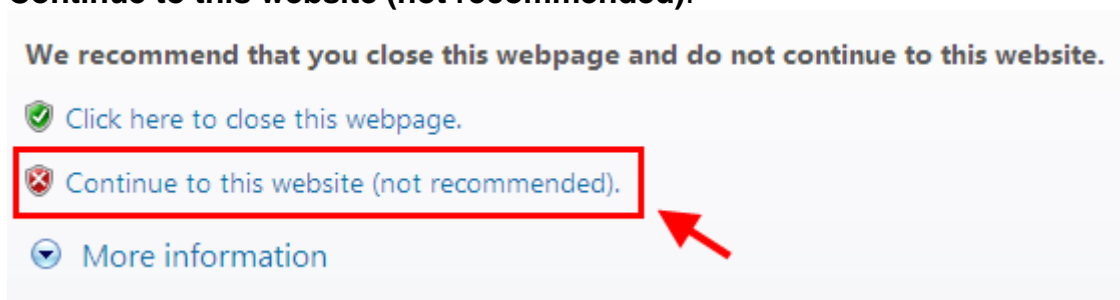


2. Click on **Go**, or press Return on your keyboard.

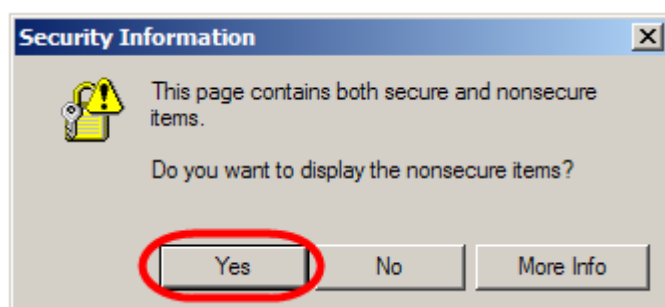
**Note:** You can also use the Web Page button in Element Manager to launch a web browser session. The BCM you wish to access must be selected in the Element Navigation Panel to do this.



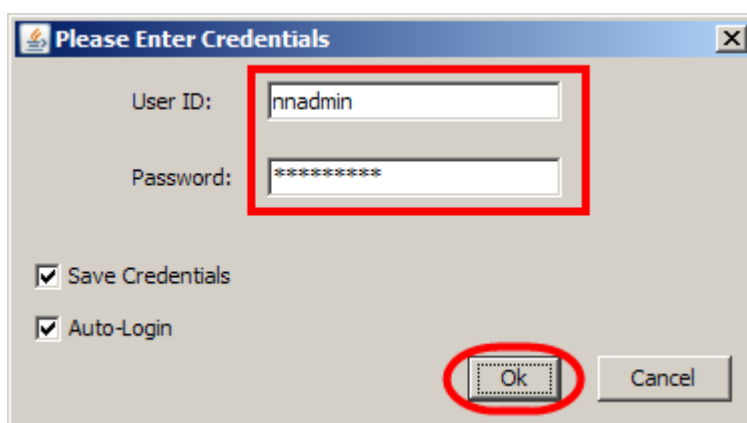
3. If you are presented with the Certificate Error window, click on **Continue to this website (not recommended)**.



4. Accept any further security messages that you may get presented with.



5. You will now see the login screen, enter your BCM User name and Password. By default these are set to User ID: nnadmin Password: PlsChgMe! Click on **OK**.

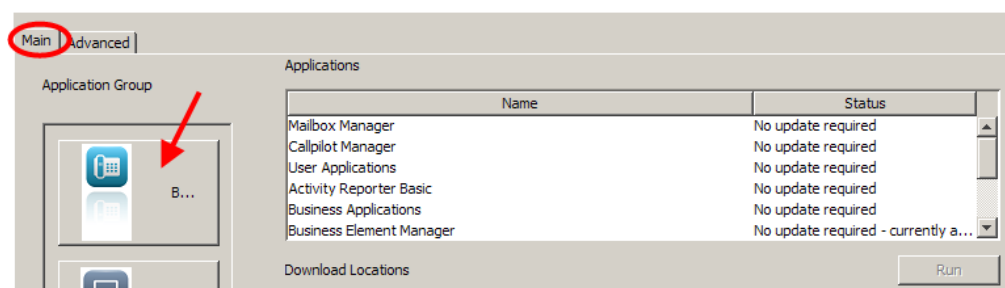


6. In the Welcome to BCM window, ensure the **Main** tab has been selected, and the **BCM** button clicked.

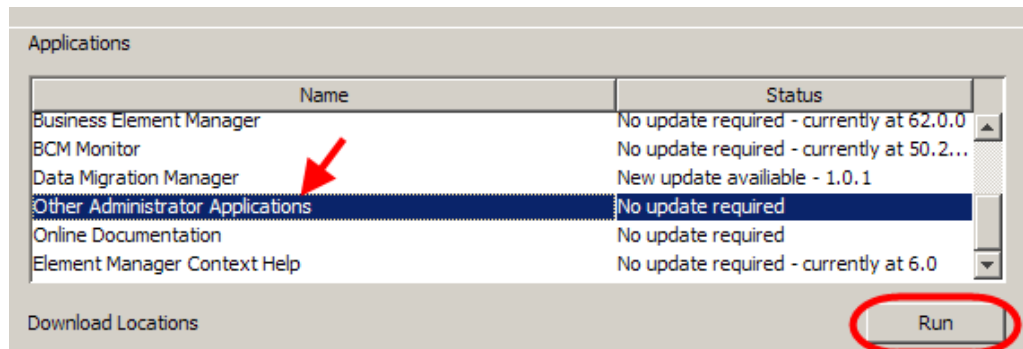
**Welcome**

to

**BCM**

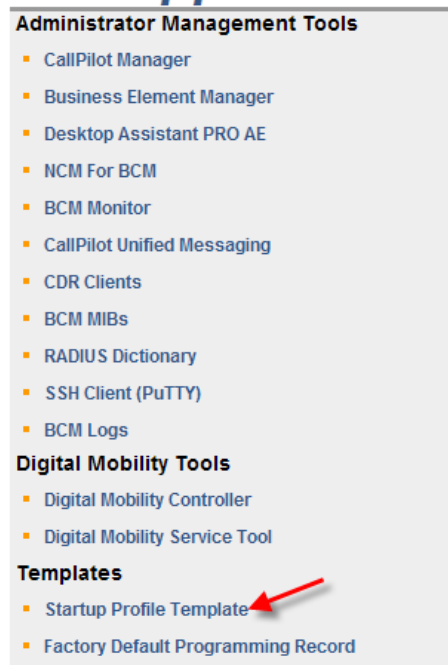


7. From the **Applications** list, select **Other Administrator Applications** and click **Run**.



8. Again, accept any security messages that appear, and if prompted enter any login details.
9. The Administrator Applications screen will be displayed.
10. Click on **Startup Profile Template**, and then **Download Startup Profile Template**.

## Administrator Applications



## Startup Profile Template

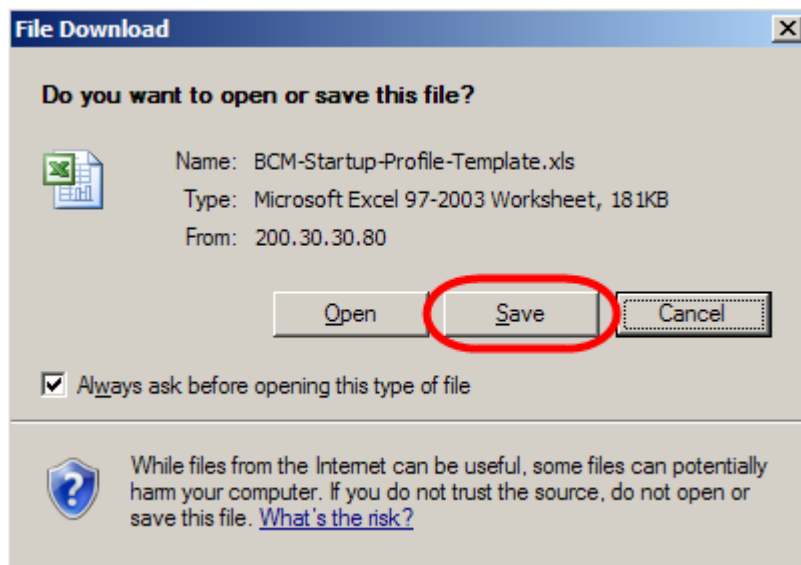
**Download Startup Profile Template**  
 See Important Notes Below

To accelerate the initial installation programming of system level parameters, a simple tool entitled "Startup Profile" can be used to quickly bring the BCM network element to a basic operational and "ready to customize" state without using Element Manager or set-based administration.

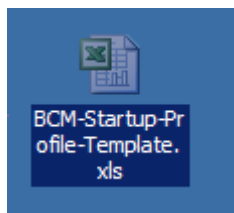
Constructed as a well-defined, easy-to-use template that can be data-filled using Microsoft Excel, the Startup profile provides a quick interface for defining parameters such as:

- system profile such as country, telephony template and key Voicemail attributes
- system IP parameters
- system level telephony attributes to automatically create the system DNs
- feature licensing information through automated application of the feature licensing file
- users and groups

11. Select the **Save** button from the **File Download** window and save the Profile template on to your PC.

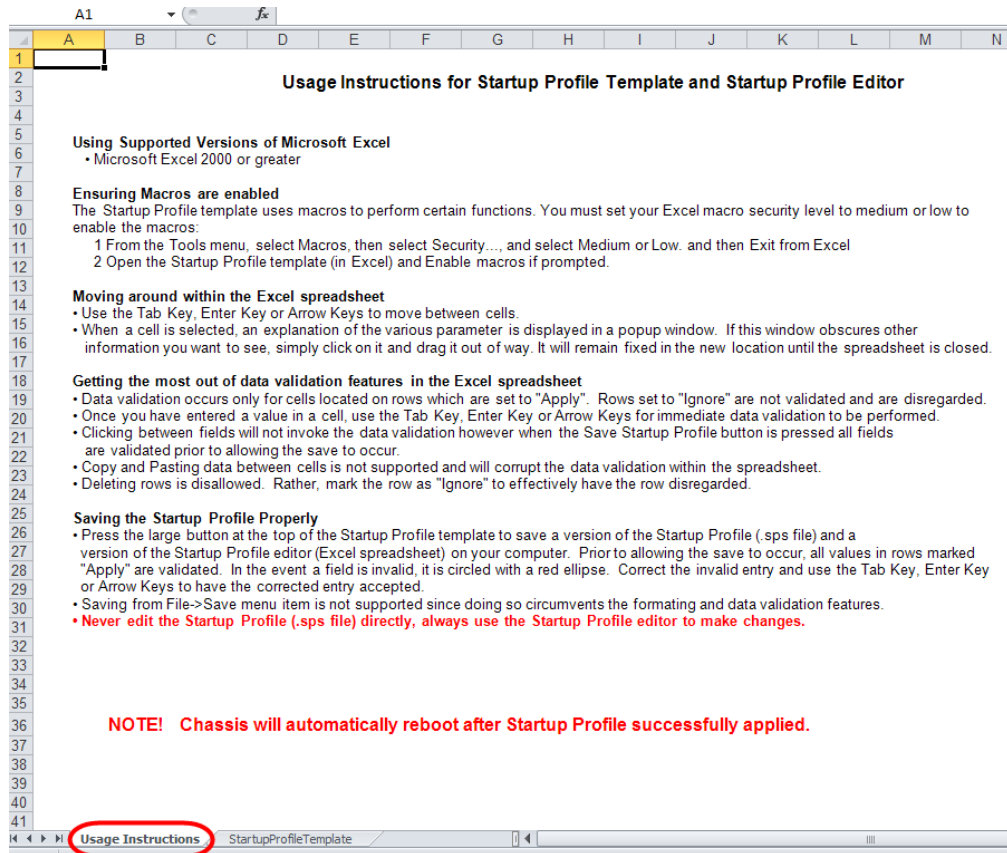


12. Once saved you can then open the file from its saved location.





13. The excel file will open from that location. You may wish to view the **Usage Instructions** page.



14. Once you have read the instructions select the **Startup Profile Template** worksheet.

**AVAYA**

Press to Save the Startup Profile (Tab Delimited File named [SystemID].sps) and associated Startup Profile Editor (Excel Spreadsheet named [SystemID].xls).

SYSTEM	ID	NAME	REGION
SYSTEM	000000000000	BCM50	North America

**TIME**

TIME	ZONE	CLOCKCONTROL	NTPSERVER	YEAR
TIME	(GMT-5:00) Eastern Time			

**DHCP**

DHCP	SERVER	GTWY	DOMAINNAME	DNS1	DNS2
DHCP	Disabled		us.avaya.com	2.2.2.2	3.3.3.3

**IP**

IP	DYNAMIC	ADDRESS	SUBNETMASK	DFLTGTWY
IP	Enabled			

**MODEM**

MODEM	STATUS
MODEM	Disabled

**KEYCODES**

KEYCODES	FILENAME
KEYCODES	validFileName.lic

**TELEPHONY**

TELEPHONY	TEMPLATE	STARTDN
TELEPHONY	DID	221

**IPTELEPHONES**

IPTELEPHONES	REGISTRATION	USEGLOBALPASSWD	GLOBALPASSWD	AUTOASSIGN	ADVERTISEMENT
IPTELEPHONES	Disabled	Disabled		Disabled	Avaya

**SNMP**

SNMP	STATUS	MINSECURITY	VERSION
SNMP	Enabled	noAuthNoPriv	v3

**SRGMAINOFFICE**

SRGMAINOFFICE	MAINFOFFICETYPE	VOIPTRUNKCODE	TESTLOCALTIMEOUT	PRIMNETADDR	ALTNETADDR	NETCONNECT
SRGMAINOFFICE	CS1000	none	2	11.11.11.11	12.12.12.12	0

Press to Insert SNMPMANAGER Row

SNMPMANAGER	IPADDRESS
SNMPMANAGER	9.9.9.9

Press to Insert SNMPCOMMUNITY Row

SNMPCOMMUNITY	STRING	PERMISSION
SNMPCOMMUNITY	public	Read Only

Press to Insert USERACCOUNT Row

Disabled User Accounts are Added with a default Password of "Time2Chgl" and Numeric Password of "864201357".

StartupProfileTemplate

## Startup Profile Settings

The following settings are entered in the Startup Profile Configuration Tool.

### System Settings

Attribute	Description
System ID	This is the System ID as stated on the System ID label on the BCM
Name	A name for the BCM system
Region	Select your region, e.g. UK.

### Time Settings

Attribute	Description
Zone	Select the Time Zone, e.g. GMT Edinburgh, London
Clock Control	Options are Core Tel, Manual, or NTP (Network Time Protocol Server)
Year	If selecting Manual, enter the current year
NTP Server	If selecting NTP, enter the IP Address of the Network Time Server

## DHCP Server

If Server is set to Enabled, you can specify the Default Gateway, DHCP Domain, and DNS Servers that will be issued to DHCP Clients

Attribute	Description
Server	Enable or Disable the core DHCP Server.
DFLTGTWY	Enter the Default Gateway on the network
Domain Name	Domain name for the DHCP Server
DNS1	Enter the Fully Qualified Domain Name or IP Address of the Primary DNS Server (if known)
DNS2	Enter the Fully Qualified Domain Name or IP Address of the Secondary DNS Server (if known)

## IP Address

These settings relate to the LAN interfaces.

Attribute	Description
Dynamic	Select Enabled to automatically receive an IP Address etc., or Disabled to specify a static address, subnet mask and default gateway.
Address	Enter the required IP Address of the LAN 1 interface.
Subnet	Enter the required Subnet Mask for the LAN 1 interface.
DFLTGTWY	Enter the Default Gateway for the LAN 1 interface.

## Modem

Select whether or not to enable the software modem, which can be used for Remote Dial-in purposes.

## Keycodes

If you have received a Keycode file and wish to apply it using the Startup Profile, enter the name of the file here. The Keycode file must be located in the root of the USB drive

## Telephony Startup Settings

Attribute	Description
Template	<b>DID:</b> Systems configured using the DID template, automatically assign target lines to all DNs. Use this template if DDI numbers are used. <b>PBX:</b> Pool A is automatically assigned for all DNs. Use this template in situations where calls are routed through an operator.
Start DN	Enter the first extensions number for your system.

## IP Telephones

Attribute	Description
Registration	Enabled or Disable IP Set registration
Use Global Password	If Yes, the IP set installer will have to enter the password set in the Global Password field
Global Password	If using Global Password, enter a password for the IP set installer to enter
Auto Assign	If Enabled, DNs will automatically be assigned to the IP sets
Advertisement	This is the display on the handset

## Other Settings

It is recommended that the rest of the settings in the Startup Profile Configuration Tool are left at default, as omitting certain fields can cause the Startup Profile to fail.

15. Continuing with the configuration, enter your BCM system ID in the **System ID field** in the Startup Profile template.

	B	C	D	E
1	<div style="text-align: center;"> </div> <div style="text-align: right; border: 1px solid black; padding: 5px;">           Press to Save the Startup Profile (Profile Editor)         </div>			
2				
3				
4				
12	SYSTEM	ID	NAME	
13	SYSTEM		BCM50	
14				
15	TIME	ZONE		
16	Apply TIME	(GMT-5:00) Eastern Time		
17				
18	DHCPSEVER	SERVER		
19	Apply DHCPSEVER	Disabled		
20				
21	IPADDRESS	DYNAMIC	ADDRESS	


**SYSTEM : ID**  
 Enter the System ID from the BCM50. Must be 12 Hexadecimal Characters in Length; Valid Chars are 0-9 and A-F.

16. The system ID can be found from within Element Manager by opening the **System folder** and selecting **keycodes** link. It can also be displayed from a BCM telephone by pressing the **Feature** key and entering **\*\*SYSID**.
17. Enter the remaining information into the Startup Profile editor that you want loaded onto the BCM. The Startup Profile editor contains explanations of the various parameters. Simply click on the cell where you want to enter information and the help text appears. You can choose which parameters to load onto your system by selecting **Apply** for the parameters you want to load. If you do not want to load certain parameters, select **Ignore**.


39		SNMPAGENT
40	Apply	SNMPAGENT
41	Apply	
42	Ignore	

18. If using a Keycode file, ensure you type in the name of the file correctly (e.g. 001158FF9B9C\_01.lic).

**Note:** The Keycode file should be copied to the root directory of the USB stick.

 **Security Warning** Some active content has been disabled. Click for more details. [Enable Content](#)

FileName

	B	C	D	E
1	 <div>Press to Save the Startup Profile (Tab De Profile Editor (Exce</div>			
2				
3				
4				
12	<b>SYSTEM</b>	<b>ID</b>	<b>NAME</b>	
13	SYSTEM	000000000000	BCM50	
14				
15	<b>TIME</b>	<b>ZONE</b>	<b>CLOCKCONTROL</b>	
16	<b>Apply</b> TIME	(GMT-5:00) Eastern Time (US & Canada)	Manual	
17				
18	<b>DHCPSERVER</b>	<b>SERVER</b>	<b>DFLTGTWY</b>	
19	<b>Apply</b> DHCPSEVER	Disabled	1.1.1.1	
20				
21	<b>IPADDRESS</b>	<b>DYNAMIC</b>	<b>ADDRESS</b>	
22	<b>Apply</b> IPADDRESS	Enabled		
23				
24	<b>MODEM</b>	<b>STATUS</b>		
25	<b>Apply</b> MODEM	Disabled		
26				
27	<b>KEYCODES</b>	<b>FILENAME</b>		
28	<b>Apply</b> KEYCODES	0011F9E61B54_7.lic		
29				
30	<b>TELEPHONYSTARTUP</b>	<b>TEMPLATE</b>		
31	<b>Apply</b> TELEPHONYSTARTUP	DID		
32				
33	<b>IPTELEPHONES</b>	<b>REGISTRATION</b>		
34	<b>Apply</b> IPTELEPHONES	Disabled		
35				
39	<b>SNMPAGENT</b>	<b>STATUS</b>	<b>MINSECURITY</b>	

**KEYCODES : FILENAME**

Enter Name of Keycode File which must reside in the Root directory of the USB Memory Device connected to BCM50.

19. Once you have entered the configuration details as outlined in the following table click the large button at the top of the Startup Profile template to save a version of the Startup Profile (.sps file) and a version of the Startup Profile editor (Excel spreadsheet) on your computer.

**Note:** You cannot copy and paste data between cells in the Startup Profile. If you attempt this, the data validation within the spreadsheet becomes corrupt. If corruption occurs, download another copy of the Startup Profile template from the BCM main unit. Also never edit the Startup Profile (.sps file) directly; always use the Startup Profile editor to make changes.

	B	C	D	E	F	G	H
1	<b>AVAYA</b>		Press to Save the Startup Profile (Tab Delimited File named [SystemID].sps) and associated Startup Profile Editor (Excel Spreadsheet named [SystemID].xls).				
12	<b>SYSTEM</b>	<b>ID</b>	<b>NAME</b>	<b>REGION</b>			
13	SYSTEM	001F9E61B54	BCM50	North America			
15	<b>TIME</b>	<b>ZONE</b>	<b>CLOCKCONTROL</b>	<b>NTPSERVER</b>	<b>YEAR</b>		
16	Apply TIME	(GMT-5:00) Eastern Time (US & Canada)	Manual				
18	<b>DHCPSEVER</b>	<b>SERVER</b>	<b>DFLTGTWY</b>	<b>DOMAINNAME</b>	<b>DNS1</b>	<b>DNS2</b>	
19	Apply DHCPSEVER	Disabled	1.1.1.1	us.avaya.com	2.2.2.2	3.3.3.3	
21	<b>IPADDRESS</b>	<b>DYNAMIC</b>	<b>ADDRESS</b>	<b>SUBNETMASK</b>	<b>DFLTGTWY</b>		
22	Apply IPADDRESS	Enabled					
24	<b>MODEM</b>	<b>STATUS</b>					
25	Apply MODEM	Disabled					
27	<b>KEYCODES</b>	<b>FILENAME</b>					
28	Apply KEYCODES	001F9E61B54_7.lic					
30	<b>TELEPHONYSTARTUP</b>	<b>TEMPLATE</b>	<b>STARTON</b>				
31	Apply TELEPHONYSTARTUP	DID	221				
33	<b>TELEPHONYSTARTUP Command Action</b>		<b>USEGLOBALPASSWD</b>	<b>GLOBALPASSWD</b>	<b>AUTOASSIGN</b>	<b>ADVERTISEMENT</b>	
34	Set to 'Apply' for command to take effect or 'Ignore' for command to be disregarded. Note: Must be set to 'Apply' when VOICEMAILSTARTUP set to 'Apply'.		Disabled		Disabled	Avaya	
39			<b>MINSECURITY</b>	<b>VERSION</b>			
40			noAuthNoPriv	v3			

20. You will be presented with warning screen below.

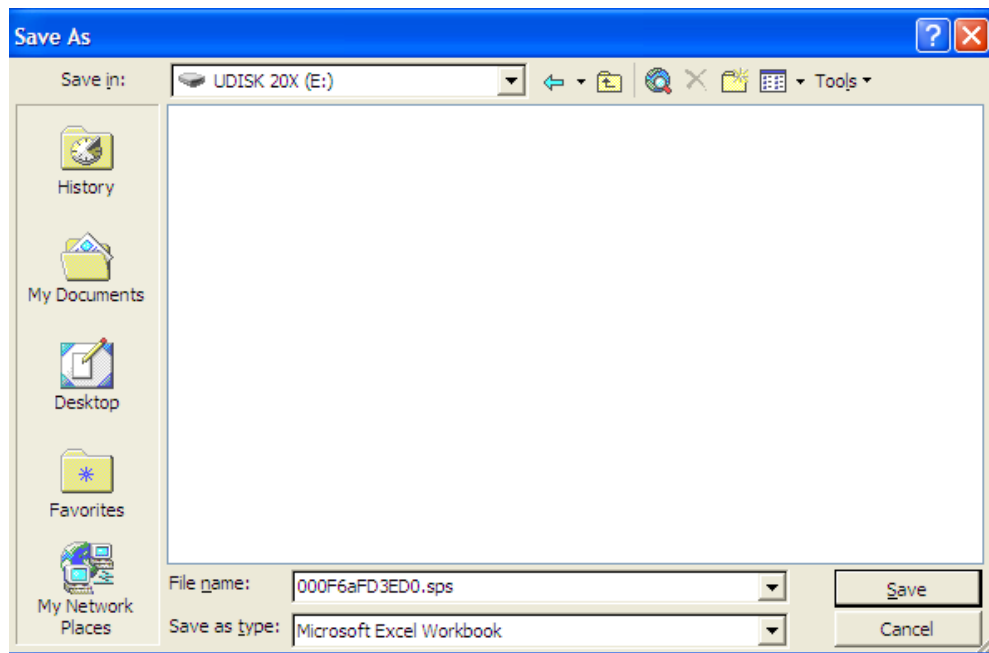
Saving Startup Profile and Associated Startup Profile Editor

OK

Cancel

You are about to be prompted to save the Startup Profile. Next, you will be prompted to save the Startup Profile Editor. Since the Startup Profile Editor is the only supported method for modifying a Startup Profile, you will find yourself in the Startup Profile Editor to make additional changes as appropriate.

21. Save a version of the Startup Profile (.sps file) on the USB memory stick. This will be noted as a drive letter in Windows Explorer.



22. The filenames for the Startup Profile editor and the Startup Profile consist of the system ID followed by the appropriate extension.
23. Exit from Microsoft Excel.

### ***Running the Startup Profile***

1. Ensure that
  - a. The BCM is turned off.
  - b. There are no data cables plugged into the BCM.
  - c. The amphenol (telephony) connector is not plugged in.
2. Insert the USB memory stick into the USB port on the front of the BCM main unit.
3. Plug in the power cable.
4. The BCM will automatically detect the USB stick, read the Startup Profile, and apply the settings to the BCM.
5. When the BCM has fully booted (both status and power lights will be fully lit), remove the USB stick and insert the telephony connector.

## **Next Step**

When the Startup Profile has been applied, you should continue with the **Media Bay Module Configuration** section of this guide.

## **Keycode Credit System**

It is now possible to remove software entitlements from one BCM and add them to a pool for distribution to other BCM systems. A Distributor or Avaya Channel Partner would manage the entitlement pool, whereas the BCM installer would apply a Keycode file sent from the Keycode supplier with a reduced set of features onto the BCM, and generate a Credit Proof File to send back to the Keycode supplier so that “liberated” Keycodes can be applied to the entitlement pool. When the Keycodes have been entered into the entitlement pool, they can be distributed to other BCM systems.

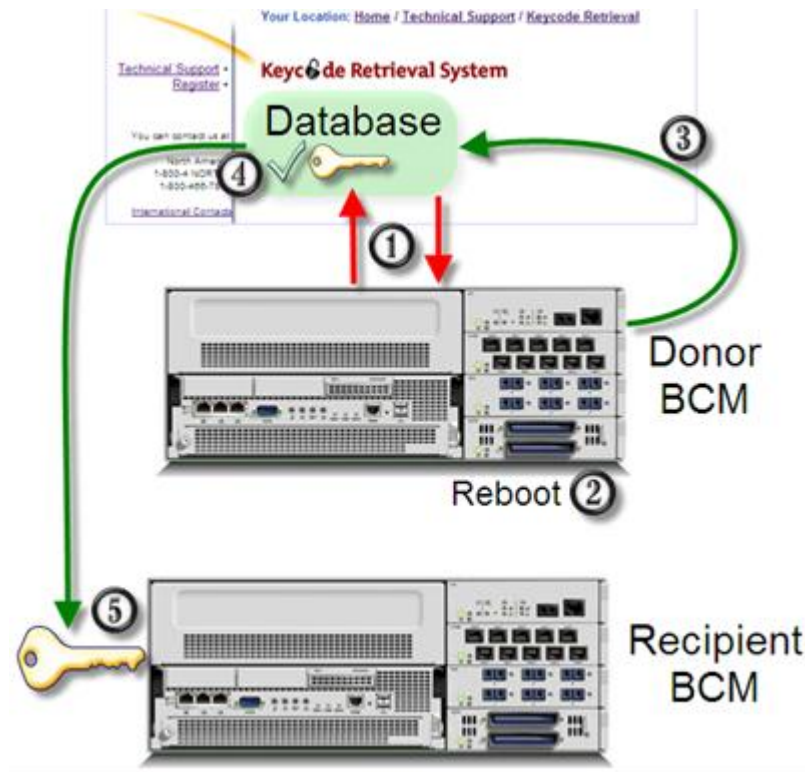
**Note:** At present, the Keycode Credit System is only applicable to BCM RIs 5.0 or later BCM's. Also, transferral of Keycodes between BCM50 and other platforms (and vice versa) is not possible.

**Note:** Entitlements can only be transferred between BCM's belonging to the same customer. Also, each BCM must be registered to the customer's entitlement pool in the Keycode Retrieval System (KRS).

An overview of the process of removing Keycodes from a donor BCM and applying these to the entitlement pool for distribution is described as follows:

1. In the Avaya Keycode Retrieval System (KRS), generate a Keycode with reduced entitlements then apply it to the donor BCM.
2. Generate a Keycode Credit Proof file and reboot the BCM (this deactivates the features on the donor BCM that you wish to transfer to other BCMs).
3. Transfer Credit Proof file to KRS to activate the credit.
4. KRS Validates the Credit proof file and the Credit becomes available to the customer.
5. The credits can be transferred to another BCM (through a new KeyCode containing the additional entitlements).





The BCM installer's responsibilities can be summarized as follows:

1. Apply the Keycode file with reduced entitlement to the donor BCM.
2. Generate a Credit Proof File on the donor BCM. The BCM will require rebooting.
3. Send the Credit Proof File to the Keycode supplier.
4. Keycode files generated from the entitlement pool are applied in the same way as regular Keycode files.

## **Avaya Documentation Links**

- [Installation and Maintenance Guide](#)
- [BCM50 Installation Checklist and Quick Start Guide](#)
- [Keycode Installation Guide](#)
- [Configuration – System](#)
- [Configuration – Devices](#)
- [Configuration – Telephony](#)